



# ArchiTech™ by Networx™

with Keypad / ProxReader

## USER'S GUIDE

© NAPCO Security Technologies, Inc. 2018

OI410LF 8/18



KEYPAD/PROXREADER



iLock™  
SMARTPHONE  
APP



RR-4BKEYFOB  
WIRELESS REMOTE  
RELEASE



PROXIMITY  
CARD



RR-1BUTTON  
WIRELESS REMOTE  
RELEASE



DL-WINDOWS™  
PROGRAMMING SOFTWARE



AL-PRE PROXIMITY CREDENTIAL  
READER / ENROLLER

ArchiTech™ by Networx™ Wireless Network Access  
Control System with Proximity Access

# ArchiTech™ by Networx™ Wireless Locks

THE ARCHITECH BY NETWORX WIRELESS ACCESS CONTROL SYSTEM IS A STATE-OF-THE-ART MICROPROCESSOR-BASED COMPUTER NETWORK PROGRAMMABLE PROXIMITY SECURITY LOCK.



**Ideal for small businesses with multiple users and multiple credential types (PIN, Prox, Bluetooth app)!**

ArchiTech™ Series Locks are an ideal access control solution, blending the advanced and robust Networx™ wireless access control system with the classic mortise lock functionality where a simple button press allows for the lock to remain in passage. ArchiTech Series Locks can be used to control access a door at a time; across a wireless network; or as an integral part of a new or existing security system -- spanning a few, or hundreds of doors, in one building, a campus or multiple sites around the world.

ArchiTech security locks are designed to allow all features to be programmed through its wireless Networx radio link from a DL-Windows-equipped computer. With "wireless" communication, physical cables are NOT required to transfer data between DL-Windows and the wireless locks. A Networx Gateway is used in conjunction with your computer to retrieve logs, download User credentials and program features into each wireless lock in the system. In addition, its real-time clock / calendar automatically adjusts for Daylight Saving Time and allows for automated programming of scheduled events. The combination **Keypad/ProxReader** allows for additional programming options and user access methods, including keypad-entered User Codes, multiple proximity credential technologies (125kHz Format, 13.56MHz Format depending on model), including proximity cards and fobs, wireless remote releases and Bluetooth LE access via the iLock™ mobile device app.

## Table of Contents

About this Manual.....	2	"Keypad Programming" Schedule Record Sheet .....	27
ArchiTech Features .....	3	"DL-Windows Mode" Operation / Features .....	28-30
Supported Products and Applications .....	4	Emergency Commands.....	31-32
Terminology Used in this Manual.....	5-6	Bluetooth Support.....	33
ArchiTech User Number Definitions .....	7	Using the iLock App.....	34-35
ArchiTech Series Design Overview.....	8	Wireless Remote Releases .....	36
Overview: Three Ways to Program .....	9	Low Battery and Battery Replacement .....	37
Power Up and Secure the Door .....	10	Erase All Programming .....	38
Select "Program Card Programming" Operation.....	11-12	Power Down -- Retain Existing Programming .....	39
"Keypad Programming": Overview of Functions .....	13	LED and Sounder Indications.....	40
"Keypad Programming" Conventions .....	14	User Card Record Sheet.....	41
"Keypad Programming" Functions.....	14-25	Glossary.....	42-43
"Keypad Programming" Record Sheet.....	26	ArchiTech Networx Limited Warranty .....	44

### About this Manual

This manual documents the programming, operation and features of the ArchiTech™ by Networx™ series wireless locks. If you are new to DL-Windows, this manual does not contain preliminary information regarding integration with DL-Windows; stop here, read the *DL-Windows User's Guide* (OI382) and the *DL-Windows for Networx User's Guide* (OI383) to become familiar with DL-Windows, then return here. Some terms you will encounter include:

- The word "**lock**" is a generic word used to indicate one of the many ArchiTech™ by Networx physical locking device models available. This physical lock may be in its normally "locked" state (preventing passage through the door) or in an "unlocked" state (allowing passage through the door).
- The word "**credential**" is also a generic word used to indicate a proximity card, a proximity "fob", a Bluetooth iLock app, a User Code, or any other type of credential that allows passage through the door.
- In the DL-Windows software, the word "**configure**" has a specific meaning--to "**configure**" is to "assign" discovered physical ArchiTech series locks to a Gateway module, thus ensuring a fixed wireless communication channel exists between selected physical locks and a selected Gateway (see page 4 and OI383 for more information about Gateways).
- The words "**pairing**", "**enrolling**" and "**programming**" may be used interchangeably.
- Take care to ensure that the terms "**fob**", "**keyfob**" or "**key fob**" are not misunderstood. The terms may refer to a **Wireless Remote Release** (such as a model RR-4BKEYFOB *Wireless Remote Release Keyfob*) or the terms may refer to a fob-shaped proximity credential (the kind usually placed on a key ring).

# ArchiTech™ Features

## Three Ways to Program

Adding keypad buttons to the proximity reader allows for additional programming options:

- **"Program Card Programming"**: For "stand-alone" operation, without enrollment into a Networx (DL-Windows) system. Create special proximity "Program Cards" at the lock's Proximity Reader, then use these "Program Cards" to create new proximity credentials for distribution.
- **"Keypad Programming"**: Programming using the keypad. After setting your unique "Master Code", add a User Code (be aware that only a User Code can lock the lock; see page 10, "**SECURING THE DOOR**", step 6), set the Date, Time, and Weekday, add credentials and program other functions described starting on page 14. Keypad Programming can be used "stand-alone" or after enrollment into a Networx system.
- **DL-Windows Mode: Full Administrative programming** from a PC using Alarm Lock's DL-Windows Software. For a description of all features, see the *DL-Windows User's Guide* (OI382) and the *DL-Windows for Networx User's Guide* (OI383). There are two ways to use DL-Windows:
  - **Networked mode**: PC running DL-Windows is connected to (wirelessly or wired) a network, either using an Ethernet or 802.11 connection. Communications are accomplished through networked Gateway module(s). See page 4 for supported products.
  - **Non-networked mode**: PC running DL-Windows does not require a network. Communications are accomplished using an **AL-IME-USB** Gateway inserted into a USB port on your Windows laptop or PC. **Note**: Only "Local" Emergency Commands are supported when using an **AL-IME-USB** Gateway. See page 4 for supported products.



## Audit Trail

- 40,000 Event Capacity (see OI382)
- Entries Logged with Time and Date (see OI382)
- Critical Programming Events Logged (see OI382)
- Door position logging capability (see "Features" Screen in OI382)
- Up-loadable using Alarm Lock's DL-Windows Software (see OI382 and OI383)

## Lock Features

- Metal Key Override for all cylindrical locks
- Non-Volatile (Fixed) Memory
- Real-Time Clock, with Automatic Daylight Saving Time Adjust (see OI382)
- Visual and Audible Feedback (see chart on page 40)
- Integrated Door position switch (see "**Door Contact Sensor**" on page 8)
- Uses four Standard AA Batteries, with Low Battery Warning indication (see chart on page 37)

## Scheduling (Using DL-Windows)

- 500 Scheduled Events (see OI382)
- Automated Unlock / Lock (see OI382)
- Enable / Disable Users (see page 5 for definition of "User")
- Enable / Disable Groups (see page 6 for definition of "Group")
- Real-Time Clock and Calendar (see OI382 and OI383)
- *Power Saving Mode*: Turns radio off to prolong battery life (see page 30)
- Bluetooth ON/OFF scheduling via DL-Windows (see page 33)\*



## User Access Methods

- Keypad-entered User Codes
- Works with Multiple Proximity Access Credential Technologies (125kHz Format, 13.56MHz Format depending on model), including Proximity Cards, Proximity "Fobs", RR-1BUTTON *Wireless Remote Release Button* (see WI1999) and the RR-4BKEYFOB *Wireless Remote Release Keyfob* (WI2004)
- Manual Card Enrollment Option for "Program Card Programming" Installation (see page 11)
- Bluetooth LE access via iLock™ Smartphone app (see page 34)\*



## User Features

- Supports up to 5000 Key-free Users (see "**What is a User?**" on page 5)
- Service Credential (see "**User 300: One-Time-Only Service Credential**" on page 6)
- Guard Tour (see "**User 298 and User 299: Guard Tour**" on page 6)
- Users Assignable to 4 Groups (see "**What is a Group?**" on page 6)
- Global Lock-Down / Unlock in emergency; activated from *Wireless Remote Release* Transmitters, DL-Windows or initiated from another Networx lock in the system (see page 31)

Wireless programming range: Up to 200 feet, depending on building construction materials.

\*For ArchiTech models equipped with Bluetooth LE technology.

# Supported Products & Applications

## AL-IM2 SERIES Gateway Modules

The ArchiTech series door lock contains a radio that transmits and receives data (via a private wireless signal) to an intermediate device called a "Gateway" interface module. In turn, this module is connected (either wirelessly or wired) to a computer network such as a LAN or corporate Intranet. A Windows PC connected to this network can control and program all ArchiTech series door locks by the use of *DL-Windows* software (see OI382 and OI383). With access rights to this software, one computer--or several--can control the software and consequently can control the devices in the system. **Note:** "Version 2" Gateways are the second generation of Networx wireless Gateways. ArchiTech door locks are still compatible with "Version 1" Gateways. Several Gateway device models are available:



AL-IM2-80211  
AL-IME2  
AL-IME2-POE



AL-IME2-EXP



AL-IME2-PIE



AL-IME-USB

- **"Wireless / Wired" AL-IM2-80211** Hardwired / Wireless Gateway Module. Supplied with its own class 2 transformer to supply power and supports connection to a network either using 802.11 or a standard Ethernet cable. This "Wireless / Wired" Gateway module has two antennas, one (internal) for the proprietary radio connection to the ArchiTech series door lock and the other (external) for 802.11 network transmissions. Ensure adequate 802.11 coverage in the area where the "Wireless / Wired" Gateway is mounted. Supports up to 63 Networx locks.
- **"Wired" AL-IME2** Hardwired Gateway Module, supports up to 63 Networx locks, connects directly to a network using a standard RJ-45 Ethernet cable. This model has one internal antenna used to transmit to the ArchiTech series door lock via an Alarm Lock proprietary radio connection. Powered with Class 2, 6VAC transformer (supplied).
- **"Power over Ethernet" AL-IME2-POE** Hardwired Gateway Module + POE (Power Over Ethernet), supports up to 63 Networx locks, connects directly to a network using a standard RJ-45 Ethernet cable and POE. This model has one internal antenna used to transmit to the ArchiTech series door lock via an Alarm Lock proprietary radio connection.
- **AL-IME2-EXP** The Networx™ **AL-IME2-EXP Expanders** extend the coverage area of **AL-IME2** series Gateways, allowing control of up to its rated maximum of 63 Networx locks per Gateway. **AL-IME2-EXP Expanders** are cost-effective, easier to wire than conventional Gateways, and feature a simplified 'Plug and Play' setup where the Networx system automatically identifies all newly powered Expanders and quickly determines the best wireless signal pathways. Up to 7 Expanders can be added to one **AL-IME2** series Gateway. Powered with Class 2, 6VAC transformer (supplied). **Note:** Expanders are also available in a 120VAC wall outlet pug-in design, part number **AL-IME2-PIE**.
- **AL-IME-USB** - USB Portable Gateway Module, virtually the same functionality of the Gateways listed above, however this highly portable and compact module connects to a standard USB 2.0 socket or greater in your Windows laptop or PC, quickly and effortlessly creating a wireless connection to your ArchiTech series door locks. Requires DL-Windows v5.2 or higher. **Note:** Only "Local" Emergency Commands are supported when using an **AL-IME-USB** Gateway.

## DL-Windows Software



Alarm Lock Trilogy Microsoft Windows-based software, v4.0 or higher, supports Trilogy Networx and Trilogy "stand-alone" locks, with single database (ArchiTech series door locks require v5.2 or higher). For use with *Free of charge* and downloadable online at [www.alarmlock.com](http://www.alarmlock.com). **DL-Windows software is the basis for the wireless lock programming interface.** Those unfamiliar with using DL-Windows, stop here and review the DL-Windows User's Guide (OI382) and the DL-Windows for Networx User's Guide (OI383).



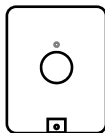
## Proximity Reader / Enroller

An **AL-PRE** is used to quickly enroll multiple proximity credentials into DL-Windows. Use the supplied 9-pin DB9 to DB9 serial cable to connect the **AL-PRE** to your computer's serial COM port. Works with most proximity credentials (37 bits or less; 125kHz).



## Proximity Credentials

ArchiTech locks work with most proximity credentials (125kHz Format, 13.56MHz Format depending on lock model).



RR-1BUTTON RR-4BKEYFOB

## RR-1BUTTON and RR-4BKEYFOB

Compatible with the **RR-1BUTTON Wireless Remote Release Button** (see W11999) and **RR-4BKEYFOB Wireless Remote Release Keyfob** (see W12004). Both can wirelessly unlock all ArchiTech Networx™ series door locks. The **RR-4BKEYFOB** is a portable pocket-size remote release, and the 1-button **RR-1BUTTON** is intended for fixed mounting at a hidden location. Each requires one battery (service life of up to 12,000 openings). During normal operation, the lock typically opens within 2 seconds of the button press.



## iLock™ Bluetooth LE Smartphone App

Android or iOS smartphone Bluetooth LE application ("app") that allows for manual remote unlock of Alarm Lock ArchiTech series devices (where equipped). For full instructions on using the iLock app, see page 34. **Note:** Up to 27 Bluetooth Users are supported for any one ArchiTech series lock.

# Terminology Used in this Manual

Before reading this section, you may wish to first read the "**ArchiTech Series Design Overview**" on page 8 to determine the manner in which you will be using your ArchiTech series lock. For more information, see the DL-Windows User's Guide (OI382) and the DL-Windows for Networx User's Guide (OI383).

## What is a Lock Program?

A Lock Program contains the instructions that an ArchiTech locking device uses to perform its various functions. Use DL-Windows (defined below) to create a Lock Program (called a "**Lock Profile**" in DL-Windows) on your computer, and then transfer and store the Lock Program in the circuitry contained inside the lock itself. The Lock Program is essentially a computer database file that maintains feature settings, proximity credential data, Schedules, Audit Trails, etc. Using DL-Windows, Lock Programs can be created with default information, edited on your PC, and then sent to (or received from) locks. The **Lock Program** consists of 4 areas: **Credential Entries**, **Features**, **Time Zones**, and **Schedules**, all defined below:

## What is a Credential?

A credential allows passage through a protected door. The word "credential" is a generic word used to indicate a proximity card, a proximity "fob", a User Code, a Bluetooth / iLock application, a Wireless Remote Release or any other type of device or design that is intended to allow the ArchiTech series lock to unlock, allowing passage through a protected door. Credentials can also be in the form of **User Codes** (also called *User Access Codes*, *passcodes*, or *PIN No. Codes*). User Codes are digits the User enters (presses) into the lock keypad to unlock the lock.

Credentials are a part of the Lock Program (defined above), and the Lock Program is stored in the lock circuitry (firmware) awaiting the Users to make use of their programmed credentials. Credentials can be added to the Lock Program and enabled, disabled, removed completely and added back in later.

## What are Features?

Your ArchiTech series lock is designed to support many options and functions. Using DL-Windows software (the **Programmable Features** screen), you can select the features you wish to activate, such as if the lock will automatically adjust for Daylight Saving Time in the spring and autumn, or if the lock sounder should be disabled or enabled. **Note:** Most features may only be added using DL-Windows.

## What are Schedules and TimeZones?

You can use the keypad or DL-Windows to add simple "Schedules" to your ArchiTech series lock. Schedules are events (recorded lock activities) that are assigned to occur automatically at specific times. For example, you can program the lock to allow certain Users access **ONLY** on Wednesdays. DL-Windows multiplies your flexibility, allowing the creation of many different combinations of Scheduled events to suit the needs of your various installations. For example, you can program the lock to allow Group 1 Users access **ONLY** during specific business hours (unlock at 9 AM, lock at noon for lunch, unlock at 1 PM, and lock again at 5 PM--every week-

day). See next page for the definition of "**Group**".

In DL-Windows, use the "**Schedule - TimeZone**" screen to first create an individual block of time called a "TimeZone" (for example, "9 AM to noon weekdays"). A TimeZone is then linked to an event to make a Schedule (for example, "unlock between 9 AM and noon weekdays"). To make Scheduling easier, DL-Windows allows TimeZones to be created, named and saved for the future, to be easily assigned to different events and added to multiple locks as needed. For more details, see the *DL-Windows User's Guide* (OI382) and the *DL-Windows for Networx User's Guide* (OI383).

## What is a User?

A User is a person who is authorized to operate the lock and/or make certain programming changes to the lock, depending on their programming abilities. Users can be anyone--from a one-time visitor in possession of a temporary credential (who will almost certainly have no authority to make changes) to the owner of the building in which the lock is installed (who will likely wish to have authority to make programming changes). The ArchiTech series locks can hold up to 5000\* Users in its programming memory; in other words, for each lock, you can have up to 5000\* Users, each in possession of a credential. **Note:** Users may be enabled, disabled or removed from locks completely, as desired.

## What is a User Number?

("User Number" = "Location Number" = "User Location" = "Slot" in Lock)

User Numbers are used primarily with DL-Windows, and are significant within each individual lock only. (ArchiTech series lock can hold up to 5000\* proximity credentials in its programming memory). Each credential can be thought of as an entry in a numbered list, up to 5000\*, maintained in the lock's internal database and in DL-Windows respectively. Each entry in this "numbered list" is represented by a User Number, and therefore proximity credential data is assigned to each "location" or "slot" in this list. When a proximity credential is assigned to a location, the credential information is stored within the Lock Program (firmware). Because Users are given credentials, it is convenient to think of each "location" as a "User", although technically the User Number is only a location within the Lock Program. In other words, it is easier to say "User 519" rather than "*The person in possession of the credential that is assigned to the User Location number 519*".

**Note:** *Where* a User is located in this list--their *User Location*--is a commonly used description of their User Number. Because of their similarities, a *User Number*, *User Location* and *Location Number* can be used interchangeably. In some DL-Windows screens, the word "Slot" is also used. All of these terms are meant to convey the same concept. See the chart, "**ArchiTech User Number Definitions**" on page 7.

## What is a "Program Card"?

"Program Cards" are created by the person responsible for programming the ArchiTech series lock when used in "**Program Card Programming**" (see page 9). Two ordinary proximity cards are provided in the factory packaging, and can be converted into "Program Cards". "Program Cards" allow for the creation of additional proximity credentials and Wireless

# Terminology Used in this Manual (cont'd)

Remote releases, activating "DL-Windows Mode" ("Network Mode"), and they also allow access (they can unlock the lock, but we do not recommend they be used as "everyday" access cards). These "Program Cards" are *unable* to be overwritten by DL-Windows because their proximity data are placed into slots 6000 and 6001 (if used, the audit trail will log them as Users 6000 and 6001). Proximity credentials assigned to User Numbers 2 through 11 are called "Administrative Users", and they possess all the functionality of these two "Program Cards". For a comprehensive understanding, see the "**ArchiTech User Number Definitions**" table on page 7.










## What is a Group?

With many lock installations, it is convenient for large numbers of similar Users to be grouped together. All of these Users might share some common attribute--for example, they may all work in the same department of a facility, or may all work the same office hours. Placing Users into Groups (by assigning them to a specific range of User Numbers) allows large numbers of Users to be controlled all at once rather than individually--saving time and effort. A typical example involves enabling or disabling a Group at a certain time (assigning them to a Schedule; for example, to allow Group "1" Users access ONLY on Wednesdays).

## How do the Emergency Commands work?

For use with all locks enrolled into the Trilogy Network™ radio network, these wireless commands can be sent to all locks in an Account during a crisis or other urgent situation.

By default, Administrative Users (Users 1-11) can send an Emergency command. In addition, any User Code can be programmed to allow the use of these Emergency Commands by simply adding that User Code to an "Emergency Users" list within DL-Windows. When an enabled User Code is pressed at any lock keypad, first the lock unlocks, then the lock permits the use of these emergency commands to be sent to all locks in the network, as follows:

- ...press    to issue "**Emergency Lock Down**", to indefinitely lock all doors;
- ...press    to issue "**Emergency Passage**", to indefinitely unlock all doors;
- ...press    to issue "**Return to Normal**" returning all doors to "normal" (non-emergency) operation.

In addition, emergency commands may be sent via an RR-4BKEYFOB. **Note:** 3 chirps sound after each emergency command entry. See page 31 and the DL-Windows User Guide OI383, "**Emergency Commands**" for more information.

**Note:** DL-Windows does not need to be running to allow these "Emergency" commands to be initiated; **any** lock keypad in the system can be used to disseminate these commands to all locks in the network.

## Who are Users 297-300?

Credentials assigned to User Numbers 297, 298, 299 and 300 have special abilities, as follows:

### User 297: Quick Enable User 300

The credential assigned to User Number 297 possesses the unique ability to enable the credential assigned to User Number 300. When credential 297 is used at the lock, credential 300 is enabled *for one time use* (allowing passage for one time only). Once used, User 300's credential is subsequently disabled.

For example, you wish to allow one-time access to a temporary worker. Simply use credential 297 at the lock and give credential 300 to the temporary worker. Later, when the temporary worker uses the credential 300, the lock unlocks to allow access through the door for one time only. Later, if the temporary worker uses credential 300 a second time, access will be denied. If you later wish to grant the temporary worker access again, simply use credential 297 again and credential 300 will be re-enabled (again, for one time only).

### User 298 and User 299: Guard Tour

A Guard Tour credential is used to log the movement of a security guard as he or she makes rounds from one assigned guard tour station to the next. Using the User 299 credential provides precise verification and accountability of a guard's movement by logging the location with a time and date stamp in the Event Log ("Audit Trail").

**Note:** Credentials assigned to User 298 and User 299 are **not** access credentials (meaning these credentials do NOT allow the security guard to pass through the door).

### User 300: One-Time-Only Service Credential

This is the credential (given to the service person) that is enabled by the credential assigned to User 297. See **User 297: Quick Enable User 300** above.

## Who are Bluetooth Users (7000-7026)

For ArchiTech series locks that contain a Bluetooth LE radio, Bluetooth credentials work just like any other type of credential, but are transmitted from the smartphone app, "iLock". Simply launch the iLock app and tap the **Unlock** button to allow entry. For more information about using Bluetooth with your lock, see page 33. **Note:** Up to 27 Bluetooth Users are supported for any one ArchiTech series lock.

## What is DL-Windows?

DL-Windows is a Microsoft Windows-based computer software program that allows you to program your ArchiTech series door lock. With DL-Windows, you can quickly create Lock Programs (called "Lock Profiles" in DL-Windows) that allow you to add multiple types of credentials, retrieve event logs, create Schedules and program many other useful features.

The benefit of DL-Windows is that it allows you to set up all lock programming in advance (on your computer), and then later send the information to the locks at your convenience. For more information about DL-Windows, see OI382 and OI383.

\* To be exact, 5000 "User Numbers" are available, though not all allow access. For a broader understanding of how these numbers are organized, see "**ArchiTech User Number Definitions**" on page 7.

# Architech User Number Definitions

## Adding Extra "Admin" Credentials

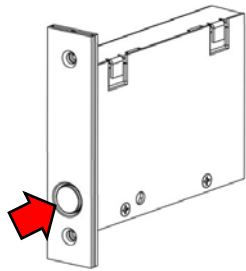
Some of the terminology in this table was originally defined in the *DL-Windows User Guide* OI382. Please refer to this manual for specific definitions. For more information, see **Terminology** on page 5 and page 6, and also see OI383. Proximity credentials assigned to User Numbers 2 through 11 are called "Administrative Users", and they possess all the functionality of the two "Program Cards" that reside in slots 6000 and 6001.

USER TYPE	USER NUMBER	FUNCTIONALITY / COMMENTS
Master Code	1	User Number 1 must be a 6-digit numeric PIN (factory default is 123456). No other credentials can be added to this slot.
Installer 1 Installer 2	2 & 3	These are Administrative Users. Programming ability (able to place lock into Enroll Mode and to enroll additional Basic User credentials or a Wireless Remote Release), Emergency User (during an Emergency state, credential can unlock the physical lock for the duration of the Pass Time).
Manager 1 Manager 2 Manager 3	4 - 6	These are Administrative Users. Programming ability (able to place lock into Enroll Mode and to enroll additional Basic User credentials or a Wireless Remote Release), Emergency User (during an Emergency state, credential can unlock the physical lock for the duration of the Pass Time).
Supervisor 1 Supervisor 2 Supervisor 3	7 - 9	These are Administrative Users. Programming ability (able to place lock into Enroll Mode and to enroll additional Basic User credentials or a Wireless Remote Release), Emergency User (during an Emergency state, credential can unlock the physical lock for the duration of the Pass Time).
Reserved ("Print Only 1") Reserved ("Print Only 2")	10 - 11	These are Administrative Users. Programming ability (able to place lock into Enroll Mode and to enroll additional Basic User credentials or a Wireless Remote Release), Emergency User (during an Emergency state, credential can unlock the physical lock for the duration of the Pass Time). <b>Note:</b> The description "Print Only" was carried over from legacy lock types, and is retained for consistency of DL-Windows screens. However, these Users have the same Administrative User abilities as Users 2-9.
Basic Users*	12 - 5000	No programming and no Administrative User abilities.
Enable User 300	297	Present credential to enable "One-Time Only Service" User (User Number 300). Includes Basic User functionality.
Guard Tour 1 Guard Tour 2	298, 299	Non-passage User (does not unlock the lock), meant to be used for logging activity. <b>Note:</b> The description "Guard Tour" was carried over from legacy lock types, and is retained for consistency of DL-Windows screens.
One-Time Only Service	300	Enabled for one-time use by User Number 297. See "Enable User 300", above.
Program "Cards" (two)	6000, 6001	Same abilities as Users 2-11 above, plus ability to perform the "DL-Windows Mode" Re-Activation procedure. Cannot be added or edited via DL-Windows software.
Bluetooth Users (first two)	7000 - 7001	Same abilities as Users 2-11 above, plus ability to perform the "DL-Windows Mode" Re-Activation procedure. Cannot be added or edited via DL-Windows software.
Bluetooth Users (additional)	7002 - 7089	No programming and no Administrative User abilities.

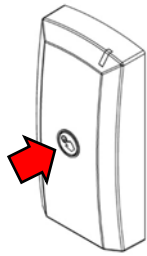
\***Note:** Additional Emergency Users may be added as required by DL-Windows. "Basic User" credentials may also be given the added ability to enter a locked door during Emergency Lock Down. In addition, all Users may be granted the ability to enter a door during Emergency Lock Down by disabling the feature "**Users are disabled during Lockdown**". See the "**Emergency Users**" section on page 32, and also OI383 for details.

# ArchiTech Series Design Overview

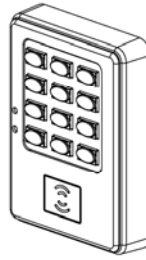
## Parts Overview (not to scale)



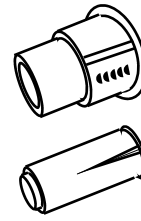
MORTISED  
NETWORK CONTROL  
UNIT



SURFACE-MOUNTED  
NETWORK  
CONTROL UNIT



KEYPAD / PROXREADER



DOOR CONTACT  
MAGNET  
(TWO TYPES)



DOOR  
CONTACT  
SENSOR

## Why Use Proximity Credentials?

With ordinary door locks, the need to make physical copies of metal keys and distributing them can be a huge organizational and financial task -- and what will you do if someone causes a security breach by losing their key?

The answer lies in the use of "firmware". Firmware exists inside your ArchiTech™ series lock, and can be changed ("programmed") to suit your changing requirements. Instead of distributing metal keys, distribute proximity cards, fobs or User Codes ("credentials"). If lost, they can easily be deleted from the lock firmware, and new ones added. (Proximity cards, proximity fobs and User Codes are the firmware equivalent of metal keys; just present a valid card to the Proximity Reader (or press your User Code at the keypad) to unlock the lock). Furthermore, credentials like cards and fobs differ from metal keys in that they are **not duplicates**-- each credential is "unique" to the lock, and therefore can easily be deleted from the lock firmware without needing to be "in hand". Another advantage is that proximity credentials cannot easily be duplicated, unlike metal keys.

## "Program / Passage" button

Much like the classic "rocker switch / stop button" found on a standard mortise lock, the ArchiTech™ Series locks feature a "Program / Passage" button allowing for sustained passage through the door without a credential (see arrows in the images above). These buttons are identical in functionality with each model and are initially used in the "POWER UP" process on page 10 or 11. During normal operation, the "Program / Passage" button is used to intentionally place the lock into a passage state as needed, without a credential. **Note:** The "Program / Passage" button is disabled when the door is closed; the door must be physically open to allow use of the "Program / Passage" button (see next section regarding the Door Contact Sensor and door position monitoring). In addition, the "Program / Passage" button is used for activating (and re-activating) "DL-Windows Mode" and for credential enrollment in "Program Card Programming". **Note:** If you wish, the "Program / Passage" button can be disabled using DL-Windows (see page 29).

## Door Contact Sensor

The **Door Contact Sensor** is required to monitor the position

of the door (open or closed). The **Door Contact Sensor** is shown above at right; note also that a Sensor is integrated within the edge of the **Mortised Network Control Unit**. With the ArchiTech series locks, DL-Windows can program the lock to log a "door position" event or "Door Ajar" event. The lock writes a "Door Ajar" event to the system log or turns on an alert sounder when the Door Contact Sensor contacts remain open past a specified time. In addition, should these contacts detect that the door was opened without first a valid credential to unlock the unit, or the door was opened without first the inside lever being turned, a "Forced Entry" (or door "kick-in") event will be logged, and an alert sounder will turn on for 5 seconds. **Note:** This "Forced Door Detection" feature, though programmable in DL-Windows, is only available for locks that possess the "RX Request to Exit" functionality.

## Emergency Commands

The ArchiTech series locks respond to **Emergency Commands** ("Emergency Lock Down", "Emergency Passage" and "Return to Normal"). In emergencies, a Lock Down command or Unlock command can set all locks to a locked or unlocked state *globally* in seconds, initiated from a Wireless Remote Release or initiated from the Network server running DL-Windows (**Note:** Emergency Passage is not available with the Wireless Remote Release). **Emergency** commands are available in two types: "Global" or "Local".

- With "Global", activating the command locks down (or places into passage) the entire system. Locks configured for "Global" also accept and adhere to an Emergency command initiated at another lock via a Wireless Remote Release.
- With "Local", activating the command does NOT lock down the entire system; only the lock that is "paired" to the Wireless Remote Release will change state (up to 4 locks).

**Note:** Locks configured as "Local" are not included in "Global" Emergency Commands sent from the Network Server running DL-Windows. For a full explanation about using Emergency Commands with your ArchiTech series lock, see "Emergency Commands" on pages 31-32. For further information about how Emergency Commands work with your *entire* system, see OI383.





# Overview: Three Ways to Program





To maintain maximum flexibility, your ArchiTech series lock can be programmed in three ways, each can be thought of as a separate programming "environment". Each are available to suit your installation requirements:

## "Program Card Programming"

Also known as "Stand-Alone Mode" when used with other ArchiTech lock models without a keypad, "Program Card Programming" permits all programming (for example adding or deleting proximity cards) to be performed using special proximity "Program Cards" at the lock's Proximity Reader. With "Program Card Programming", the lock is NOT enrolled into a DL-Windows Network system (namely "DL-Windows Mode", described above). Later, if you wish, your lock can be enrolled into a Network system by performing the "**DL-WINDOWS MODE RE-ACTIVATION**" procedure on page 12. **IMPORTANT:** All proximity credentials added with Program Card Programming *will be deleted* upon the locks' enrollment into a DL-Windows Network system. To use Program Card Programming, turn to page 11.

## "Keypad Programming"

With the addition of a keypad to the ArchiTech series door locks, programming User Codes and other features can be performed using button presses at the Keypad/ProxReader, and simplifies programming for those more familiar with the traditional way of programming Alarm Lock door locks. The **Keypad/ProxReader** keypad contains 12 buttons, numbers 1 through 9 plus zero, a star button () and a special "AL" button (). After the "**POWER UP**" procedure has been performed (page 10 or 11), Keypad Programming may be used either **before** or **after** the lock is enrolled into a DL-Windows Network system (namely "DL-Windows Mode", described above). Each of the various programming "Functions" are described, starting on page 13. However, before you can start to program your lock using the keypad, you must first enter something called "Program Mode". In Keypad Programming, there are only two "modes"--"Normal Mode" and "Program Mode". You enter "Program Mode" to use the keypad to make changes to the lock program; when you finish programming and wish to put the lock into use, you exit "Program Mode" to enter "Normal Mode".

You enter Program Mode using the keypad by pressing the **Master Code** of the lock that was set at the factory (then wait for the green light and press  until multiple beeps are heard). The Master Code is basically a secret 6-digit "passcode" that allows you to enter Program Mode. But since all locks are identical and leave the factory with the same Master Code, this factory Master Code is therefore not very secret--and should be changed to your own personal Master Code. This way, only YOU can enter Program Mode and make changes to the lock programming. Once the new Master Code is set, then you can program other things using the keypad, such as setting the weekday, date and time. After this, you can start entering User Codes for people to use. All changes to the lock are organized by their Function Number. Want to change the date? Use Function Number 38 (page 18). Want to add a new User Code? Use Function Number 2 (page 14). There are 99 Functions in total, some that you may use often, and others that you may never need. Notice also that when you program your lock, programming tends to follow a consistent 5-step pattern: (1) Enter Program Mode (2) Press  followed by the Function # (3) Press  and enter data (4) Press  to end (5) Exit Program Mode to put the lock into use.

## "DL-Windows Mode"

Also called "Network Mode", this mode refers to the standard operation of the ArchiTech series lock after it is enrolled into a Network system (i.e. configuration by the DL-Windows software). All programming is performed using DL-Windows software (version 5.2 or later). By default, after the "**POWER UP**" procedure has been performed (page 10 or 11), your ArchiTech series lock is available for discovery by any Network Gateway and by DL-Windows for a 24 hour "window" of time. DL-Windows communicates with a Gateway module (models listed on page 4) to wirelessly communicate with the lock's internal radio. See the *DL-Windows for Network User's Guide* (OI383) for more information about Gateways, and see page 28 for "DL-Windows Mode" operation. There are two ways to use DL-Windows:

- **Networked mode:** PC running DL-Windows is connected to (wirelessly or wired) a network, either using an Ethernet or 802.11 connection. Communications are accomplished through networked Gateway module(s). See page 4 for supported products.
- **Non-networked mode:** PC running DL-Windows does not require a network. Communications are accomplished using an **AL-IME-USB** Gateway inserted into a USB port on your Windows laptop or PC. **Note:** Only "Local" Emergency Commands are supported when using an **AL-IME-USB** Gateway. See page 4 for supported products.

## ArchiTech Series Battery Life Maximization (Turns the radio off)

The ArchiTech series locks are equipped with a battery pack containing four (4) standard AA type alkaline batteries, allowing for a 2-5 year life span. To achieve maximum battery life, the ArchiTech series locks allows for an advanced feature called **Power Saving Mode** whereby an automatic Schedule can be created in DL-Windows to toggle the Mode on or off on a daily/weekly basis. **IMPORTANT:** During **Power Saving Mode**, proximity credentials WILL function normally, **but ALL communications, including Wireless Remote Releases, will NOT function.** For more information, see "**Power Saving Mode ON / OFF**" on page 30.

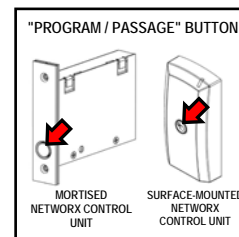
# Power Up and Secure the Door

**Remember:** The default state before and after power up is in passage ("unlocked"). If you need to secure the door ("lock the lock"), perform the "**POWER UP**" and the "**SECURING THE DOOR**" procedures, below.

## POWER UP

After physically installing your lock, you **must** perform the following "**POWER UP**" procedure for correct lock operation.

1. With the batteries disconnected, *press* and firmly *hold* the "**Program / Passage**" button for 15 seconds (button location dependent on model, see illustration at right).
2. Release the "**Program / Passage**" button and reconnect the batteries. Listen for a chirp and 3 beeps.
3. Press and hold the "**Program / Passage**" button again until you hear multiple beeps, then release the button.
4. The lock will continue to beep and flash the red LED while residual programmed data clears and the lock initializes. A final two beep/green flash sequence will occur, indicating successful completion of the power up procedure. **Note:** This step can take up to 15 seconds.



At this point, by default the ArchiTech series lock is in passage ("unlocked") and is available for discovery by any Network Gateway and by DL-Windows for the next 24 hours. **WARNING:** Because any Gateway can discover (and thus control) the lock, we recommend not to power the lock until you either perform the "**SECURING THE DOOR**" procedure (below) or perform the mode selection process (one of the options listed on page 9). **Note:** *The lock will remain in passage indefinitely (even after several years and the batteries are drained) and will **only** re-lock upon the presentation and acceptance of a valid credential.*

## SECURING THE DOOR ("LOCKING THE LOCK")

The default state before and after power up is in passage ("unlocked"). If you need to secure the door ("lock the lock"), perform the "**POWER UP**" procedure (above) first, then use the keypad to perform all of the steps on this page, below:

### Enter "Program Mode" and Change Factory Master Code

1. Press the default Master Code:      .
2. Wait for the green light and press and hold  until multiple beeps are heard. You are now in "Program Mode". **Note:** The lock will beep every 6 seconds as a reminder that you are in "Program Mode".
3. Enter a new personal 6-digit Master Code number by pressing the following keys:  
   [new Master Code]  [new Master Code]  (the second set of digits must be exactly the same).

(For example, if you want your new Master Code to be "664433". Press:

.

Now that the Master Code has been changed, there is no need to change it again (unless you want to).

### Add a User Code

4. Press       [press a new 3-6 digit User Code] .

Since you are still in Program Mode, you can repeat step 4 and add another User Code.

5. **Exit Program Mode:** Hold down any key until you hear multiple beeps. The lock is now in "normal" mode (i.e. the lock is now "in use"). **Note:** If no keys are pressed when in Program Mode, the lock will exit Program Mode after 3 minutes. A steady tone will sound for the final 15 seconds of the 3 minute timeout period as a warning. To remain in Program Mode, simply press any key.
6. **Secure the door!** There's one final step: Simply press the new User Code that you added in step 4. Listen for the lock mechanism to cycle (it's already unlocked), then after 3 seconds listen for the lock to lock. **Congratulations!** The door is secured, and will remain secured indefinitely until acted upon.

**Note:** Be aware the new User Code added in step 4 is residing in User Number 12 (see page 5 for the definition of "User Number". Simply be aware of this information, as it may become relevant later.

If you wish, write your new 6-digit Master Code here:

— — — — —

If you wish, write your new 3-6 digit User Code here:

— — — — —

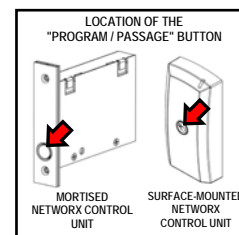
# Select "Program Card Programming" Operation

Also known as "Stand-Alone Mode" when used with other ArchiTech lock models without a keypad, "Program Card Programming" permits all programming (for example adding or deleting proximity cards) to be performed using special proximity "Program Cards" at the lock's Proximity Reader. With "Program Card Programming", the lock is NOT enrolled into a DL-Windows Network system (namely "DL-Windows Mode", described on page 28). Later, if you wish, your lock can be enrolled into a Network system by performing the "**DL-WINDOWS MODE RE-ACTIVATION**" procedure, below. **IMPORTANT:** All proximity credentials added with Program Card Programming *will be deleted* upon the locks' enrollment into a DL-Windows Network system. **Note:** If you decide to only use your Bluetooth-enabled device as a credential (no proximity cards or keyfobs), once added, the programming "environment" automatically changes to this "Program Card Programming".

## POWER UP

After physically installing your lock, you **must** perform the following "**POWER UP**" procedure for correct lock operation (the following is identical to "**POWER UP**" on page 10, and is duplicated here for your convenience).

1. With the batteries disconnected, *press* and firmly *hold* the "**Program / Passage**" button for 15 seconds (button location dependent on model, see illustration at right).
2. Release the "**Program / Passage**" button and reconnect the batteries. Listen for a chirp and 3 beeps.
3. Press and hold the "**Program / Passage**" button again until you hear multiple beeps, then release the button.
4. The lock will continue to beep and flash the red LED while residual programmed data clears and the lock initializes. A final two beep/green flash sequence will occur, indicating successful completion of the power up procedure. **Note:** This step can take up to 15 seconds.



## PROGRAM CARD CREATION / ENROLLMENT

Have the two ordinary proximity cards (supplied) ready and *in your hands* before proceeding.

1. **Enter Enroll Mode:** Press and release the "**Program / Passage**" button once (Enroll Mode = continuous beeping with green LED flashes). **Note:** Enroll Mode will continue for 30 seconds before timing out (ending).
2. Present the first proximity card to the **Proximity Reader**. Listen for 2 short confirmation beeps.
3. Present the second proximity card to the **Proximity Reader**. Again, listen for 2 short confirmation beeps.  
If the second card is not enrolled within the 30 second time out, simply press the "**Program / Passage**" button once to re-start Enroll Mode (with a new 30-second time out).
4. **Exit Enroll Mode:** Press and firmly hold the "**Program / Passage**" button for 4 seconds until you hear a series of beeps. **Note:** The lock remains in passage (unlocked).

What were two ordinary proximity cards are now two "Program Cards". You **MUST** test each card, as follows:

5. Present the first of the two "Program Cards". Listen for the lock mechanism to cycle (it's already unlocked), then after 3 seconds listen for the lock to lock. **Note:** Prior to this point, the lock has always remained in passage (unlocked), but now will remain secured (locked) indefinitely, unless acted upon.
6. Present the second of the two "Program Cards". Again, ensure the lock motor cycles and re-locks (placing the lock into its "normal" locked state). Either of these two identical "Program Cards" can now be used to enroll additional User access credentials (see page 12). You may wish to consider marking these two "Program Cards" in some way, to allow you distinguish them from other proximity cards. **Important:** We do not recommend using the "Program Cards" as your "every day" access credentials (therefore these two "Program Cards" should be kept in a safe place).

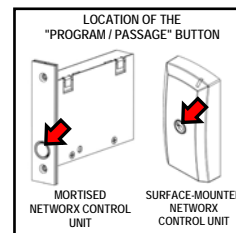
At this point, the ArchiTech series lock is (and will remain) in a locked state, two identical "Program Cards" have been created and are enrolled, and the lock is no longer available to be discovered by a Network system (24 hour window is closed). If you later wish to make the lock available to be discovered by a Network system (i.e. you wish to activate "DL-Windows Mode"), simply follow the "**DL-WINDOWS MODE RE-ACTIVATION**" procedure on the next page. **Note:** The data for the two "Program Cards" have been placed into User Number 6000 and 6001, and cannot be deleted using DL-Windows; to delete this data, use keypad Function 2 or Function 99 (using the keypad on the Keypad/ProxReader or the virtual keypad within the Bluetooth app), or by performing the "**Erase All Programming**" procedure on page 38. The next section describes how to use this "Program Card Programming" to add a credential.

(continued)

# Select "Program Card Programming" Operation (cont'd)

## ADD A CREDENTIAL

To manually add additional proximity credentials, you **MUST** first create / enroll two "Program Cards"; if you have not done so, stop here and perform the **PROGRAM CARD CREATION / ENROLLMENT** detailed above. **Note:** If you are enrolling multiple proximity cards, it is a good idea to have all of the cards you wish to enroll handy and ready. *Also, be careful not to confuse your two "Program Cards" with your other cards!*



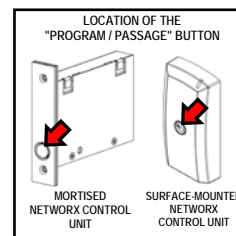
1. Open the door (and keep it open).
2. Present either one of the two "Program Cards" to the Keypad/ProxReader.
3. Within 3 seconds, press and release the "**Program / Passage**" button. Listen for a series of tones (entering "Enroll Mode"), followed by continuous beeping with green LED flashes ("in Enroll Mode and waiting for a proximity card or other proximity credential type"). Within 20 seconds perform the next step:
4. Present a proximity credential to the Proximity Reader. Upon successful credential enrollment, observe a "Valid Read" indication (two green LEDs and two beeps; the chart on page 40 lists all "**LED and Sounder Indications**").
5. Repeat step 3 for each additional proximity credential you wish to add. Each time an additional credential is added, the lock grants you another 20 seconds to present the next credential. If the 20 second time-out expires (or if a credential fails to be added or read), simply press/release the "**Program / Passage**" button and the 20 second Enroll Mode timeout duration will restart.
6. After adding your last credential, press and hold the "**Program / Passage**" button for 4 seconds until you hear a series of beeps ("Exit Enroll Mode" indication).

All added credentials are considered "Basic Users" (i.e. no programming abilities, cannot enter "Enroll Mode" and therefore cannot be used as "Program Cards"). If Wireless Remote Releases are to be used with "Program Card Programming" and/or for Emergency Lock Down, please read "**Understanding "Global" vs. "Local"**" on page 31 and "**Wireless Remote Releases**" on page 36.

## DL-WINDOWS MODE RE-ACTIVATION

If the 24 hour window for discovery by DL-Windows has expired, **or** if you wish to migrate from "Program Card Programming" to "DL-Windows Mode", you may do so by restoring the lock to its original factory condition (see **Erase All Programming** on page 38) or by performing the following procedure:

To make the ArchiTech series lock available for discovery by DL-Windows version 5.2 or later (re-activate "DL-Windows Mode"), use your previously created "Program Cards" as follows:



1. With the door open, present one of the previously created "Program Cards" to the Proximity Reader.
2. Press and hold the "**Program / Passage**" button for 6 seconds until the Proximity Reader LED flashes green twice and beeps twice.
3. Release the "**Program / Passage**" button.

**Note:** While the "**Program / Passage**" button is being held down in step 2, the door will remain unlocked for the length of the button press.

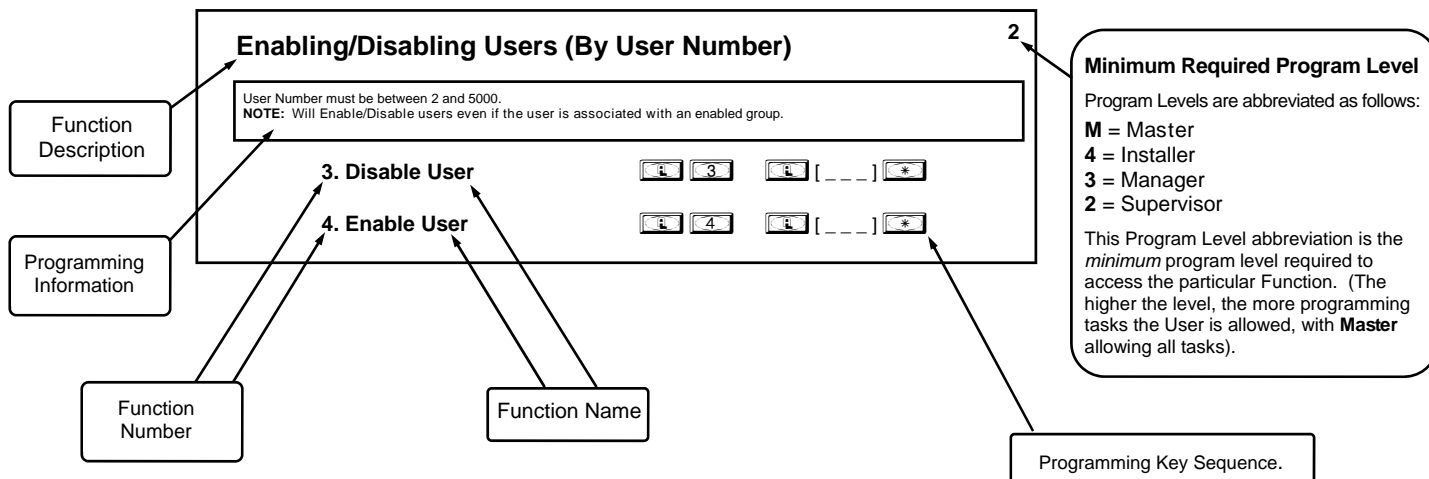
The ArchiTech series lock is now available for discovery by DL-Windows. **WARNING! Cards and other credentials added in "Program Card Programming" will be deleted!**

# "Keypad Programming": Overview of Functions

Function 1	Change Master Code	See page 14
Function 2	Add/Delete/Change User Codes	See page 14
Function 3	User Disable (By User Number)	See page 15
Function 4	User Enable (By User Number)	See page 15
Function 5	Reserved	--
Function 6	Enable Total User Lockout	See page 15
Function 7	Disable Total User Lockout	See page 15
Function 8	Exit Program Mode	See page 15
Function 9	Enable User 300 (Service Code)	See page 15
Function 10	Erase All Users Except the Master Code	See page 15
Function 11	Reserved	--
Function 12	Clear All Schedules and Timeout Functions	See page 16
Function 13	Reserved	--
Function 14 - 17	Group 1-4 Disable	See page 16
Function 18	Disable All Groups	See page 16
Function 19 - 22	Group 1-4 Enable	See page 16
Function 23	Enable All Groups	See page 16
Function 24	Reserved	--
Function 25 - 29	Reserved	--
Function 30 - 33	Reserved	--
Function 34	Reserved	--
Function 35	Group Add/Delete Association	See page 17
Function 36	Reserved	--
Function 37	Expiration Date for Bluetooth	See page 17
Function 38	Set Date	See page 18
Function 39	Set Time	See page 18
Function 40	Set Weekday	See page 18
Function 41	Daylight Saving Time Start Date	See page 18
Function 42	Daylight Saving Time End Date	See page 18
Function 43	Speed Up Clock	See page 19
Function 44	Slow Down Clock	See page 19
Function 45 - 46	Passage Mode Enable/Disable	See page 19
Function 47	Reserved	--

Function 48	Enable Passage Mode	See page 20
Function 49	Disable Passage Mode	See page 20
Function 50	Return Lock to Normal Passage Mode Schedule	See page 20
Function 51	Passage Mode Configuration	See page 20
Function 52 - 54	Pass Time	See page 20
Function 55	Enable 30 Second Smart Pass	See page 21
Function 56	Reserved	--
Function 57	Reserved	--
Function 58	Reserved	--
Function 59	Reserved	--
Function 60	Number of Attempt Before Lockout	See page 21
Function 61	Set the Attempts Lockout Time	See page 21
Function 62 - 63	Reserved	--
Function 64	Disable Remote Input	See page 21
Function 65	Enable Remote Input Pair Wireless Remote Release	See page 21
Function 66	Reserved	--
Function 67	Program System Features	See page 22-24
Function 68	Default All System Features	See page 24
Function 69 - 70	Enable/Disable Enter Key	See page 25
Function 71	Reserved	--
Function 72 - 73	Scheduled Enable/Disable Passage Mode	See page 25
Function 74 - 77	Schedule Enable Group 1 - 4	See page 25
Function 78	Schedule Enable All Groups	See page 25
Function 79 - 82	Schedule Disable Group 1 - 4	See page 25
Function 83	Schedule Disable All Groups	See page 25
Function 84 - 87	Reserved	--
Function 88	Reserved	--
Function 89	Reserved	--
Function 90	Reserved	--
Function 91	Reserved	--
Function 92	Reserved	--
Function 93	Reserved	--
Function 94	Reserved	--
Function 95 - 98	Reserved	--
Function 99	Clear All Lock Programming	See page 25

# "Keypad Programming" Conventions



## General Program Mode Information

If a wrong key is pressed during code entry, press the [ ] key until the error sound is heard (7 short beeps), this will clear the entry. Re-enter the key sequence again.

All program sequences are followed by the [ \* ] key; 2 short beeps indicate a successful program sequence.

# "Keypad Programming" Functions

## USERS

### 1. New Master Code (User Number 1)

[ ] [ 1 ] [ ] [ \_ \_ \_ \_ \_ ] [ ] [ \_ \_ \_ \_ \_ ] [ \* ]

(New Master Code) (Confirm New Master Code)

- Master Code must be 6 digits-only.
- Master Code is Keypad Code Access only (see page 9 for more information about Master Codes).
- **Factory Default** = [ 1 ] [ 2 ] [ 3 ] [ 4 ] [ 5 ] [ 6 ]

**M**

### 2. Adding and Deleting User Codes and/or Proximity Credentials (for User Numbers 2-5000)

(Entering a "User Code" / "PIN No. Code" into the lock programming)

[ ] [ 2 ] [ ] [ \_ \_ \_ \_ ] [ ] [ \_ \_ \_ \_ \_ ] [ \* ]

(User Number) (User Code)

(Entering a Proximity Credential)

[ ] [ 2 ] [ ] [ \_ \_ \_ \_ ] [ \* ] [Beep Beep Beep]

(User Number) (Present credential to reader within 10 seconds)

(Deleting Entire User)

[ ] [ 2 ] [ ] [ \_ \_ \_ \_ ] [ \* ] [Beep Beep Beep]

(User Number) (Wait 10 seconds for beeping to end)

- User Number must be between 2 and 5000.
- User Code must be 3-6 digits.
- Each User Code can be thought of as a person. With each person in possession of their own unique User Code, managers can control access to the lock by adding or deleting User Codes. See "What is a User Number?" on page 5.

**3**

# "Keypad Programming" Functions (cont'd)

## USERS (Continued)

### User Enable/Disable (By User Number)

- User Number must be between 2 and 5000.

**NOTE:** Will Enable/Disable Users even if the User is associated with an enabled Group. Use Function 3 to disable a specific User Number and their associated User Code. If the disabled User Code is entered, the lock will flash 1 Green and 4 Red Flashes (with 1 long and 5 short beeps) indicating that the User Code exists in memory, but is disabled. Function 4 will "undo" Function 3.

2

#### 3. Disable User



#### 4. Enable User



### 5. Reserved

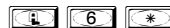
### User Lockout Mode

Prevents all User Codes (Except User 1 Code) from operating the lock. **Note:** No other programming functions or schedules (including a DL-Windows data transfer) will re-enable Users. Users must be re-enabled with Function 7. **Note:** Does not change the User enable/disable status. **Note:** If the lock is currently in Passage Mode (door "unlocked") and Function 6 is programmed, the lock will remain in Passage Mode.

M

#### 6. Enable Total User Lockout Mode

*(This Function enabled through keypad only)*



#### 7. Disable Total User Lockout Mode

*(This Function enabled through keypad only)*



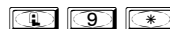
#### 8. Exit Program Mode



Allows Program Mode exit for keypads without hold-down functionality, such as some Wiegand readers with integral keypads.

3

#### 9. Enable User 300 (Service Code)



Service Code is a One-Time-Only Code. Once it is used, it is disabled until enabled again.

**NOTE:** User Number 297 is used to reset Service Code Use. See "Terminology Used in this Manual" on page 6 for more information and examples regarding special Users 297-300.

2

#### 10. Erase All Users Except the Master Code (User 1)

*(This Function enabled through keypad only)*



Erases all User Codes except the Master Code (User 1).

- Function 10 can only be performed using the keypad.

M

### 11. Reserved

# "Keypad Programming" Functions (cont'd)

## CLEAR FUNCTIONS

### 12. Clear All Schedules and Timeout Functions



Function 12 clears all programmed *Schedules* and all *Timeout Functions*. (To clear All Timeout Functions only, see Function 13 below). Function 12 will clear all of the following: All Schedule Functions 72 through 93, Timeout Functions 5, 25 through 34 and Function 47. **Note:** Function 12 also resets Passage Mode and any disabled Groups. After using Function 12, your Scheduled/Timeout features must be manually re-programmed.

3

**NOTE:** Up to 4 Timeout Functions may be pending at any one time. An error beep will sound when attempting to program more than 4 Timeout Functions. This Function only disables the timeout; the event associated with the timeout will remain.

### 13. Reserved

## GROUPS

### Group Enable/Disable

Enter the functions below to Enable/Disable Groups. Functions 14 - 23 will each override existing scheduled events. Therefore, Functions 14 - 23 are temporary, take effect immediately, and are always overridden by future scheduled events that already exist within the lock programming.

2

#### 14. Disable Group 1



#### 15. Disable Group 2



#### 16. Disable Group 3



#### 17. Disable Group 4



#### 18. Disable All Groups



#### 19. Enable Group 1



#### 20. Enable Group 2



#### 21. Enable Group 3



#### 22. Enable Group 4



#### 23. Enable All Groups



### PRIORITY ORDER

1. Disabled Users
2. Enabled Groups
3. Disabled Groups
4. Enabled Users

The Priority Order details which Function will take effect before ("have priority over") others. For example, as per the list above, Enabled Users have the lowest priority, and other Functions can affect the status of these Users. Disabling a Group (Functions 14-18) will take priority over the enabled Users in that Group, disabling them. Enabling Groups (Functions 19-23) will take priority over those tasks lower in the list, and finally disabling a User (Function 3) takes priority over all other tasks listed.

### 24. Reserved









# "Keypad Programming" Functions (cont'd)

25 - 34. Reserved

## GROUPS

**NOTE:** Clear All Timeout Functions by entering Function 13.

### 35. Group Add/Delete Association

    [ \_ \_ \_ ]  [ \_ \_ \_ \_ ]  \*

(User Number) (Groups)

As per the chart on page 7, the lock's default programming from the factory associates certain User Numbers with certain Groups. To override these default Group associations, Function 35 manually associates (or disassociates) a selected User with a selected Group. During programming, Groups not selected are then disassociated from the User. Function 35 is helpful when the number of Users you wish to add to a Group outgrows the number of User Numbers defaulted to a Group (50); or if an existing User joins a department and you wish to simply add them to a Group.

- User Number must be between 2 and 5000; Groups 1-4 (to associate with User) may be selected.

**Add Example:** To associate User 67 with Groups 1, 2 and 4;

Enter:                       \*

**Delete Example:** To remove all Group associations for User 67;

Enter:                       \*







**NOTE:** If a User is associated with more than one Group, **all** associated Groups would have to be disabled before the User is disabled.

3

36. Reserved

## BLUETOOTH SUPPORT

### 37. Expiration Date for Bluetooth

    [ \_ \_ \_ ]  [ \_ \_ \_ \_ \_ ]  \*

(User Number must be 7002+) (MMDDYY)

Used with J and T "style" ArchiTech series locks that contain Bluetooth LE technology to allow for entry via a smartphone app (see page 33 for details). Feature 37 allows you to disable Bluetooth connectivity for a single user at midnight on a specific date. **Note:** Only the last two digits of the year are currently supported, therefore entering a date prior to the current date will immediately disable Bluetooth connectivity. For example, entering "00" for the "YY" year will designate the year 2000, and will therefore immediately disable Bluetooth connectivity.

**IMPORTANT:** Only User Numbers 7002 and greater are valid for this command.

3

# "Keypad Programming" Functions (cont'd)

## CLOCK SETTINGS

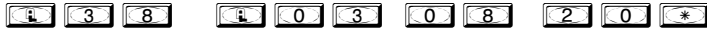
### 38. Set Date



- Use Month Day Year format - MMDDYY - Single digit months and days are entered with a preceding zero.
- Enter ONLY the last two digits of the year.

3

**For Example:** March 8, 2020; Enter:



### 39. Set Time



- Time must be 4 digits
- Use 24 Hour Format (add 12 hours to program PM time)

3

**For Example:** To set time to 8:25PM;

Enter: [0] [3] [9] [ ] [0] [2] [0] [2] [ ] [5] [\*]

**For Example:** To set time to 8:25AM;

Enter: [0] [3] [9] [ ] [0] [8] [2] [5] [\*]

### 40. Set Weekday



- For day enter: 1 for Sunday, 2 for Monday, 3 for Tuesday, 4 for Wednesday, 5 for Thursday, 6 for Friday and 7 for Saturday.

3

**For Example:** To set day to Sunday;

Enter: [0] [4] [0] [ ] [1] [\*]

### 41. Daylight Saving Time Start Date



The manner in which Daylight Saving Time (DST) is observed varies with location, therefore the DST adjustment is fully flexible to accommodate these regional differences. Function 41 allows the entry of a *DST Start Date* (month, day and week), and Function 42 allows the entry of a *DST End Date* (month, day and week). DST begins and ends at 2AM on the programmed date. Enter [0] [4] [1] [ ] [0] [0] [0] [ ] [0] [\*] to disable DST. All locks leave the factory with DST enabled and pre-programmed to the following start and end dates (for the USA beginning 2007):

4

- **Default DST Start Date:** March, Week 2, Sunday ("Second Sunday in March")
- **Default DST End Date:** November, Week 1, Sunday ("First Sunday in November")

To program the DST start date using the keypad, press: [0] [4] [1] [ ] [ M M W D ] [\*] where "M M W D" represents:

- **"M M" = Two digits of the month** (01 through 12 = January through December. Single digit months are entered with a preceding zero).
- **"W" = Single digit for "week of the month"** (valid entries are 1-5 where "1" is the first week, "2" is the second week, "3" is the third week, "4" is the fourth week and "5" is the last week of the month).
- **"D" = Day of the week** (valid entries are 1-7: 1 for Sunday, 2 for Monday, 3 for Tuesday, 4 for Wednesday, 5 for Thursday, 6 for Friday and 7 for Saturday).

Example: To set the default start date of "second Sunday in March", press:

[0] [4] [1] [ ] [0] [3] [2] [ ] [1] [\*] (03 = "March", 2 = "2<sup>nd</sup> week", 1 = Sunday).

### 42. Daylight Saving Time End Date



End date of Daylight Saving Time (month, week, day). Enter [0] [4] [2] [ ] [0] [0] [0] [ ] [0] [\*] to disable DST. See Function 41 for full explanation.

4

# "Keypad Programming" Functions (cont'd)

## CLOCK ADJUST

### Clock Adjust

Number of seconds to adjust (speed up/slow down) the clock each day must be between 0-55 seconds. 4

**Note:** Repeated use of these Functions are not "cumulative" (this means, for example, if the clock has *already* been set to speed up 10 seconds per day, and then is found to need an additional 10 seconds, then program 20 seconds using Function 43).

**Example 1:** Clock is losing 13 seconds every day, enter:

4 3 1 3 \*

This example assumes that the Clock Adjust setting was at the factory default of zero.

**Example 2:** Clock is gaining 13 seconds every day, enter:

4 4 1 3 \*

This example assumes that the Clock Adjust setting was at the factory default of zero.

**Example 3:** To set the clock adjust setting back to the factory default of zero, enter:

4 3 \* or 4 4 \*

#### 43. Speed Up Clock

(This Function enabled through keypad only)

4 3

[ \_ \_ ] \*

(seconds)

#### 44. Slow Down Clock

(This Function enabled through keypad only)

4 4

[ \_ \_ ] \*

(seconds)

### Clock Accuracy

The internal oscillator is factory calibrated to an accuracy of  $\pm 5$  minutes/year. Changes in ambient temperature may affect accuracy. If necessary, the accuracy of the internal clock may be adjusted by first updating the correct time via Function 39. After an interval of about 1 month, re-set the correct time via Function 39 and then view the Audit Log. Because the Audit Log displays both the "New Clock Time" and the "Old Clock Time", a daily accuracy (in seconds) can be determined by taking the difference in seconds between the "Old" and "New" times divided by the number of days between the two Function 39 entries. **Note:** Because the minimum available adjustment is 1 second per day, the inaccuracy of the clock must exceed about 6 minutes per year before adjustment is necessary.

## PASSAGE MODE

### Passage Mode Enable/Disable - Schedule will Override

- Function 45 allows passage through the door without the need for a credential. Re-Lock using Function 46. 2
- Programmed Schedules will override the state of the lock when Functions 45 and 46 are used. If it is required that programmed schedules do not override Passage Mode, enable/disable Passage Mode using Functions 48/49. **Note:** Because of the temporary nature of these features, Functions 45-46 can only be enabled using the keypad.

#### 45. Enable Passage Mode

(This Function enabled through keypad only)

4 5 \*

#### 46. Disable Passage Mode

(This Function enabled through keypad only)

4 6 \*

# "Keypad Programming" Functions (cont'd)

## PERMANENT PASSAGE MODE

### Passage Mode Enable/Disable - Schedule will not Override

- Function 48 allows passage through the door without the need for a credential. Re-Lock using Function 49.
- Programmed Schedules will not override the state of the lock using functions 48 and 49. If it is required that programmed schedules override Passage Mode, Enable/Disable Passage Mode using Functions 45/46. Use Function 50 to "undo" Functions 48 and/or 49, and therefore return the lock to all pre-existing scheduled functions. **Note:** Functions 48-50 can only be enabled using the keypad. **Warning:** Function 49 will inhibit all scheduled Passage Mode events.

2

#### 48. Enable *Permanent Passage Mode*

(This Function enabled through keypad only)



#### 49. Disable *Permanent Passage Mode*

(This Function enabled through keypad only)



#### 50. Return Lock to Normal Passage Mode Schedule

(This Function enabled through keypad only)

(Locks will lock or unlock depending on the current schedule). Use Function 50 to "undo" Functions 48 and/or 49, and therefore return the lock to all pre-existing scheduled functions.



**NOTE:** See Scheduled functions 72 and 73 for Scheduled Passage Mode.

### 51. Passage Mode Configuration



(Mode)

- **Mode 1 (Normal):** Passage Mode must be enabled/disabled using Function 45 and 46. **Mode 1 (Normal) is the factory default.**
- **Mode 2:** Group 2 toggles Passage Mode.
- **Mode 3:** Group 2 enables, Group 3 disables Passage Mode. Disable Passage Mode has priority if User is a member of both Groups 2 and 3.

With **Mode 2**, each time any member of Group 2 enters their User Code, they will toggle Passage Mode. For example, if Passage Mode is enabled, and a Group 2 User enters their User Code, Passage Mode will be disabled. If a few seconds later they enter their User Code again, Passage Mode will be enabled. With **Mode 3**, Group 2 members will always enable Passage Mode, and Group 3 members will always disable Passage Mode. For example, if Passage Mode is already enabled, and a Group 2 User enters their User Code, the Passage Mode status will not be changed due to the Function 51 Mode 3 configuration. If Passage Mode is already enabled, and a Group 3 User enters their User Code, Passage Mode will become disabled.

4

## PASS TIME

### Pass Time

The Pass Time is the length of time the lock stays unlocked after a valid User Code is entered (or proximity credential presented). When the Pass Time expires, the lock will re-lock automatically. Use the functions below to change the Pass Time to 3, 10 or 15 seconds. **The Pass Time is defaulted to 3 seconds.** **Note:** Compare to Function 55, "Enable 30 Second Smart Pass" on next page.

4

#### 52. Set Pass Time to 3 Sec.



#### 53. Set Pass Time to 10 Sec.



#### 54. Set Pass Time to 15 Sec.



# "Keypad Programming" Functions (cont'd)

## SMART PASS

### 55. Enable 30 Second Smart Pass



#### Smart Pass

Enabling this feature overrides the existing Pass Time and sets the duration to 30 seconds. Therefore, after a valid credential has been presented, the ArchiTech series lock will remain unlocked for 30 seconds OR until the door opens or closes. **Note:** The above function is dependent upon the door position (a Door Contact Sensor is required).

4

### 56 - 59. Reserved

## LOCKOUT

### 60. Number of Attempts Before Lockout



(Number of Attempts)

- Number of attempts before lockout must be 1-9 attempts.
- The number of attempts is reduced by half every time the keypad is locked out without a successful code entry (default is 6 attempts).
- The attempt count is reset each time a valid code is entered.

4

### 61. Set the Attempts Lockout Time



(Lockout Time)

- Lockout Time must be 1-60 seconds.
- How long the keypad is locked-out after a series of unsuccessful attempts (default is 18 seconds).

4

### 62-63. Reserved

## REMOTE INPUT

### Remote Input / Wireless Remote Release Pairing

- Wire a Normally Open Contact to Wires (White & White). Momentarily close switch to unlock door to allow person to pass through door.
  - Enter the functions below to Disable/Enable the Remote Input.
- NOTE:** The Remote Input is enabled as part of the default program.

2

### 64. Disable Remote Input



### 65. Enable Remote Input



**Note:** In addition to using a wired momentary switch, Function 65 is also used to pair a compatible Wireless Remote Release such as the **RR-1BUTTON** (see W11999) or the portable pocket-size **RR-4BKEYFOB** (see W12004). Function 64 is also used to remove all paired Wireless Remote Releases from the locking device. *Be aware of the potential loss of Wireless Remote Release pairing(s) that can result from using Function 64.* Refer to the above WIs for complete instructions.

### 65. Pair Wireless Remote Release



Slot Number  
(1-10)

### 66. Reserved

# "Keypad Programming" Function 67

## 67. Program System Features



4

- Use Function 67 to program **one or more** system features. For example, program to disable the sounder.
- Before you implement any of the following Function 67 system features, take note that some features are enabled ("ON") by default (for example, see #39, below). If you wish to turn a Function 67 system feature *off* that is either enabled "ON" by default or was enabled manually, we strongly recommend that you first be aware of all other Function 67 system features that may have already been programmed, because the ability to "toggle" a single Function 67 system feature "ON" or "OFF" is not supported. First, all features must be turned "OFF" by performing a special Function 67 command called "**Set All Function 67 Features to OFF**", i.e. , then simply re-enable all of your previously programmed system features.
- Be aware of another, similar, special Function called "**Default All System Features**" (Function 68, i.e. ). When a manually enabled Function 67 system feature is no longer desired, use this Function 68 command to restore all defaults, resulting in some being set to "OFF", and some "ON" (depending upon their respective default states). **Note:** Since the use of the Function 67 "**Set All Function 67 Features to OFF**" or the Function 68 "**Default All System Features**" commands may require restoring previously implemented system features, it is recommend to complete the "**Keypad Programming Record Sheet**" on page 26 in order to keep track of your settings.

## System Options

24. **One Time Entry for Group 3 Users.** When programmed, a Group 3 User is allowed entry only once, then becomes disabled. **Note:** When the credential is entered for the first time and access is granted, the Event Log will show "Entry" followed by "User Disabled". If the User Code is entered a second time, access will be denied, and the Event Log will show "User Denied Access". **Note:** To assign the selected User Codes to Group 3, see Function 35 on page 17.
25. **Disable Sounder.** All audible feedback is disabled (except when in Program Mode and when **Enable Sounder on Emergency** [Function 67, option 43] is enabled). For a summary of lock activities that trigger the sounder, see "**LED and Sounder Indicators**" on page 40.

## Remote Input Features

For more information about using the Remote Input, see page 21 (Function 64 and Function 65).

29. **Toggle Passage Mode.** Wireless Remote Release toggles Passage Mode. See page 36 to pair a Wireless Remote Release to your lock. **Note:** This Wireless Remote Release setting; "Toggle Passage Mode" and the Function 67, feature 58 setting named "**Enable Toggle Mode (Manual Relock)**" that is described on page 24 are two independent settings. The Remote Release operation is not affected by the Function 67, feature 58 setting.
36. **Cancel Passage on Button Press.** Used with feature 58 ("**Toggle Locked / Unlocked**", see below), if enabled, when the state of the lock is in Passage (i.e. "unlocked"), one press and release of the "**Program / Passage**" button on the Network Control Unit will change the state of the lock to "locked" (Passage is cancelled).

## Emergency Command Options

Local Emergency Command Options (45 and 47, described below) are enabled ("ON") by default. Global Emergency Command Options (38, 46 and 48, described below) can be enabled below or by a subsequent DL-Windows download. **Note:** For more information about "Global" vs. "Local" Emergency Commands, see page 31.

(continued)

# "Keypad Programming" Function 67 (cont'd)

## 67. Program System Features (cont'd)



38. **Lock Responds to "Global" Emergency Commands.** (Default = OFF, thus default = Lock responds to "Local" Emergency Commands only). Allows lock to respond to lock down requests initiated by Network server running DL-Windows or another lock (as opposed to directly from a Wireless Remote Release).
39. **Users are Disabled During Lockdown.** (Default = ON). Basic Users (User Numbers 12 - 5000) are denied access (passage through the door) during an Emergency.
43. **Enable Sounder on Emergency.** (Default = OFF) Integral sounder beeps for 30 seconds while in Emergency.
47. **Activate Local Emergency: Keyfob initiates Local Emergency Commands.** (Default = ON). Initiating an Emergency command from a Wireless Remote Release (for example model RR-4BKEYFOB *Wireless Remote Release*) places only the paired lock into an Emergency state; the Emergency command is not sent to other locks in the system.
48. **Activate Global Emergency: Keyfob initiates Global Emergency.** (Default = OFF). Initiating an Emergency command from a Wireless Remote Release (for example model RR-4BKEYFOB *Wireless Remote Release*) immediately sends the Emergency command to all other locks in the system, then places the paired lock into an Emergency state.

## Door Status Monitoring

40. **Enable Door Monitoring.** (Default = OFF). If the Door Position Contacts remain open past the time set at Function 68 "Door Ajar Trip Time" (default is 20 seconds), a Door Ajar event will be logged. See "Door Ajar" in glossary.
41. **Sounder Alert on Door Ajar.** (Default = OFF). The integral sounder beeps when the Function 68 "Door Ajar Trip Time" expires. Feature 40 must be set ("ON") for this sounder to operate (follows default Door Ajar Trip Time of 20 seconds unless programmed otherwise using Function 68).
42. **Forced Door Detection.** (Default = OFF). If a Forced Door is detected, i.e. the Door Position Contacts detect the door was opened without first a valid credential unlocking the lock, or the door was opened without first the inside lever turned (to activate an internal Lever Monitor Switch), a Forced Door event will be logged, the sounder will beep for 3 seconds, and the red LED will turn on. See "Forced Door" in glossary. Feature 40 must be set ("ON") to enable Forced Door Detection.
56. **Automatic Deadbolt (No Passage Override).** Enable when automatic deadbolt hardware is used. **Note:** Be aware of the following terminology when reading the descriptions for feature 56 and 57: The state of the door can be "open" or "closed". The state of the monitored automatic deadbolt can be "extended" or "retracted". The state of the ArchiTech lock can be "unlocked" or "locked". If the ArchiTech lock is "unlocked", Passage Mode is enabled, allowing both the inside and outside levers to retract the latch. If the ArchiTech lock is "locked", Passage Mode is disabled, and the outside lever "rigid" (unable to be turned), with the inside lever remaining mechanically connected to allow the retraction of both the latch and deadbolt when turned.

With automatic deadbolt hardware, the deadbolt automatically extends when the door closes. If this feature 56 is enabled, whenever the deadbolt extends, the ArchiTech lock will *a/ways* change to a "locked" state.

**Example:** A door is equipped with an automatic deadbolt and feature 56 is enabled. The door is closed, the ArchiTech lock is "locked" and the deadbolt is extended. A user inside the protected premises turns the inside handle thus retracting both the ArchiTech lock latch and deadbolt. The user opens the door and exits the premises. When the door closes, the automatic deadbolt extends, and the ArchiTech lock goes into a "locked" state. To re-enter the premises, the user must use a valid credential.

**Note:** What will happen if an automatic deadbolt is installed but feature 56 is NOT enabled? The result will be an inability to permanently enable Passage Mode. If feature 56 is not enabled and you decide to enable Passage Mode, the first time that automatic deadbolt extends, the enabled Passage Mode will be overridden (disabled), thus securing the door. Therefore, if you have an automatic deadbolt, be sure to enable feature 56. See feature 57, below, for an optional modification to this feature 56.

57. **Enable One-Time Entry Option.** Read and understand feature 56, above, before proceeding. The intent of this feature 57 is to prevent user lockout for "one time only", for doors equipped with an automatic deadbolt. This feature 57 slightly modifies feature 56 (therefore feature 56 must also be enabled for this feature 57 to operate). As stated

# "Keypad Programming" Function 67-68 (cont'd)

## 67. Program System Features (cont'd)



(Feature Number)

above, when feature 56 is enabled, and whenever the deadbolt extends, the ArchiTech lock will *a/ways* change to a "locked" state. Enabling feature 57 allows the user to press the "**Program / Passage**" button before exiting to allow the ArchiTech lock to remain in an "unlocked" state, even when the door closes and the automatic deadbolt extends for the first time; the external lever will remain mechanically connected to the deadbolt / latch to allow re-entry, and will only re-lock upon either a subsequent retraction and extension of the deadbolt, or upon a valid credential. This feature is best explained using the following step-by-step example:

**Example:** A door is equipped with an automatic deadbolt and features 56 and 57 are enabled. The door is closed, the ArchiTech lock is in a "locked" state and the deadbolt is extended. A user inside the protected premises turns the inside lever, simultaneously causing the ArchiTech latch and deadbolt to retract. The user opens the door, presses the "**Program / Passage**" button\*, and exits the premises. When the door closes, the automatic deadbolt extends for the first time, and the ArchiTech lock remains in an "unlocked" state for the duration of this first deadbolt extension. At this point, the user may re-enter the premises by simply turning the outside handle (thus simultaneously retracting both the deadbolt and latch). If the user does re-enter the premises, upon door closure the automatic deadbolt will extend for the second time and the ArchiTech lock will go into a "locked" state. Presumably the user will be inside the premises, but does not need to be; if the user chooses to remain outside the premises during the second deadbolt extension, a valid credential will be required to allow entry. **IMPORTANT:** The user **MUST** press the **Program / Passage** button to activate this **Enable One-Time Entry Option**; if the button is not pressed, the lock will relock when the door closes.

58. **Enable Toggle Mode (Manual Relock).** The intent of this feature is to prevent user lockout by always toggling either permanent "locked" or permanent "unlocked". When the current state of the lock is "locked" and this feature is enabled, either a valid credential or the turning of the inside handle will always cause the lock to remain in Passage ("unlocked") permanently. The lock may subsequently be locked ("Passage disabled") by either a valid credential or by pressing the "**Program / Passage**" button on the Network Control Unit. Compatible models only. See feature 36, "**Cancel Passage on Button Press**".

\*or presses the Remote Release button (must be configured independently for Remote Release / Toggle Mode).

## Disable All System Features

- This special Function 67 command will set all system features to "OFF" (disabled), regardless of their individual default settings. This Function exists because some Function 67 features are "ON" by default, and cannot be toggled "OFF"; the only way to turn them off is to use this Function. Compare this to Function 68. **4**

## 67. Set All Function 67 Features to OFF



## Clear (Default) All System Features

- Function 68 will "clear" all Function 67 system features by setting them all to their factory **default** states. **4**

## 68. Default All System Features





# "Keypad Programming" Functions (cont'd)

## Enter Key

- When this Function is enabled, the User must press after any valid User Code entry. Therefore, this Function allows User Codes to be subsets of other User Codes. Examples:

4

can be a valid user code;

can be a valid user code within the same lock.

(Hold ) for Master User Code to enter Program Mode.

69. Enable as Enter Key

70. Disable as Enter Key

71. Reserved

## Scheduled Passage and Group

**Note:** Clear All Schedule and Timeout Functions by entering Function 12. To set the time, see Function 39.

Use the functions below to enable Passage Mode and enable/disable Groups at the time programmed.

3

- For day enter: 1 for Sunday, 2 for Monday, 3 for Tuesday, 4 for Wednesday, 5 for Thursday, 6 for Friday, 7 for Saturday, 8 for Monday to Friday, 9 for Saturday and Sunday, and 0 for all days of week.

### Passage Mode

72. Schedule Enable Passage Mode ("Unlock")

[ \_ ]  
(Day)

[ \_ \_ \_ \_ ]   
(Time)

73. Schedule Disable Passage Mode ("Lock")

[ \_ ]  
(Day)

[ \_ \_ \_ \_ ]   
(Time)

### Groups

74. Schedule Enable Group 1

[ \_ ]  
(Day)

[ \_ \_ \_ \_ ]   
(Time)

75. Schedule Enable Group 2

[ \_ ]  
(Day)

[ \_ \_ \_ \_ ]   
(Time)

76. Schedule Enable Group 3

[ \_ ]  
(Day)

[ \_ \_ \_ \_ ]   
(Time)

77. Schedule Enable Group 4

[ \_ ]  
(Day)

[ \_ \_ \_ \_ ]   
(Time)

78. Schedule Enable All Groups

[ \_ ]  
(Day)

[ \_ \_ \_ \_ ]   
(Time)

79. Schedule Disable Group 1

[ \_ ]  
(Day)

[ \_ \_ \_ \_ ]   
(Time)

80. Schedule Disable Group 2

[ \_ ]  
(Day)

[ \_ \_ \_ \_ ]   
(Time)

81. Schedule Disable Group 3

[ \_ ]  
(Day)

[ \_ \_ \_ \_ ]   
(Time)

82. Schedule Disable Group 4

[ \_ ]  
(Day)

[ \_ \_ \_ \_ ]   
(Time)

83. Schedule Disable All Groups

[ \_ ]  
(Day)

[ \_ \_ \_ \_ ]   
(Time)

84 - 98. Reserved

### CLEAR ALL PROGRAMMING

99. Clear All Lock Programming  
(This Function enabled through keypad only)

Clears all programming, and returns lock to factory default settings. Audit Trail contents are maintained.

M

# "Keypad Programming" Record Sheet

Default Values are shown in parentheses.

Function Number(s)	Function Name	Programming																																																
43/44	Clock Adjust	+/- <table border="1" style="display: inline-table; vertical-align: middle;"><tr><td style="width: 20px; height: 20px;"></td><td style="width: 20px; height: 20px;"></td></tr></table> 0-55 (0) (0) Seconds																																																
52/53/54	Pass Time	(3 sec) <input type="checkbox"/> 10 sec <input type="checkbox"/> 15 sec <input type="checkbox"/>																																																
60	Set Lockout Attempts	<table border="1" style="display: inline-table; vertical-align: middle;"><tr><td style="width: 20px; height: 20px;"></td></tr></table> 1-9 Attempts (6)																																																
61	Set Lockout Time	<table border="1" style="display: inline-table; vertical-align: middle;"><tr><td style="width: 20px; height: 20px;"></td><td style="width: 20px; height: 20px;"></td></tr></table> 1-60 seconds (1) (8)																																																
64/65	Remote Input Momentary	(Enable) <input type="checkbox"/> Disable <input type="checkbox"/>																																																
67	Add Function 67 System Features	<table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th colspan="3" style="text-align: center;">Check all that apply:</th> </tr> </thead> <tbody> <tr> <td style="width: 5%;">24.</td> <td style="width: 85%;">One Time Entry for Group 3 Users</td> <td style="width: 10%; text-align: center;"><input type="checkbox"/></td> </tr> <tr> <td>25.</td> <td>Disable Sounder</td> <td style="text-align: center;"><input type="checkbox"/></td> </tr> <tr> <td>29.</td> <td>Toggle Passage Mode</td> <td style="text-align: center;"><input type="checkbox"/></td> </tr> <tr> <td>36.</td> <td>Cancel Passage on Button Press</td> <td style="text-align: center;"><input type="checkbox"/></td> </tr> <tr> <td>38.</td> <td>Lock Responds to "Global" Emergency Commands</td> <td style="text-align: center;"><input type="checkbox"/></td> </tr> <tr> <td>39.</td> <td>Users are Disabled During Lockdown</td> <td style="text-align: center;"><input type="checkbox"/></td> </tr> <tr> <td>43.</td> <td>Enable Sounder on Emergency</td> <td style="text-align: center;"><input type="checkbox"/></td> </tr> <tr> <td>47.</td> <td>Activate Local Emergency: Keyfob initiates Local Emergency Commands</td> <td style="text-align: center;"><input type="checkbox"/></td> </tr> <tr> <td>48.</td> <td>Activate Global Emergency: Keyfob initiates Global Emergency</td> <td style="text-align: center;"><input type="checkbox"/></td> </tr> <tr> <td>40.</td> <td>Enable Door Monitoring</td> <td style="text-align: center;"><input type="checkbox"/></td> </tr> <tr> <td>41.</td> <td>Sounder Alert on Door Ajar</td> <td style="text-align: center;"><input type="checkbox"/></td> </tr> <tr> <td>42.</td> <td>Forced Door Detection</td> <td style="text-align: center;"><input type="checkbox"/></td> </tr> <tr> <td>56.</td> <td>Automatic Deadbolt (No Passage Override)</td> <td style="text-align: center;"><input type="checkbox"/></td> </tr> <tr> <td>57.</td> <td>Enable One-Time Entry Option</td> <td style="text-align: center;"><input type="checkbox"/></td> </tr> <tr> <td>58.</td> <td>Enable Toggle Mode (Manual Relock)</td> <td style="text-align: center;"><input type="checkbox"/></td> </tr> </tbody> </table>	Check all that apply:			24.	One Time Entry for Group 3 Users	<input type="checkbox"/>	25.	Disable Sounder	<input type="checkbox"/>	29.	Toggle Passage Mode	<input type="checkbox"/>	36.	Cancel Passage on Button Press	<input type="checkbox"/>	38.	Lock Responds to "Global" Emergency Commands	<input type="checkbox"/>	39.	Users are Disabled During Lockdown	<input type="checkbox"/>	43.	Enable Sounder on Emergency	<input type="checkbox"/>	47.	Activate Local Emergency: Keyfob initiates Local Emergency Commands	<input type="checkbox"/>	48.	Activate Global Emergency: Keyfob initiates Global Emergency	<input type="checkbox"/>	40.	Enable Door Monitoring	<input type="checkbox"/>	41.	Sounder Alert on Door Ajar	<input type="checkbox"/>	42.	Forced Door Detection	<input type="checkbox"/>	56.	Automatic Deadbolt (No Passage Override)	<input type="checkbox"/>	57.	Enable One-Time Entry Option	<input type="checkbox"/>	58.	Enable Toggle Mode (Manual Relock)	<input type="checkbox"/>
Check all that apply:																																																		
24.	One Time Entry for Group 3 Users	<input type="checkbox"/>																																																
25.	Disable Sounder	<input type="checkbox"/>																																																
29.	Toggle Passage Mode	<input type="checkbox"/>																																																
36.	Cancel Passage on Button Press	<input type="checkbox"/>																																																
38.	Lock Responds to "Global" Emergency Commands	<input type="checkbox"/>																																																
39.	Users are Disabled During Lockdown	<input type="checkbox"/>																																																
43.	Enable Sounder on Emergency	<input type="checkbox"/>																																																
47.	Activate Local Emergency: Keyfob initiates Local Emergency Commands	<input type="checkbox"/>																																																
48.	Activate Global Emergency: Keyfob initiates Global Emergency	<input type="checkbox"/>																																																
40.	Enable Door Monitoring	<input type="checkbox"/>																																																
41.	Sounder Alert on Door Ajar	<input type="checkbox"/>																																																
42.	Forced Door Detection	<input type="checkbox"/>																																																
56.	Automatic Deadbolt (No Passage Override)	<input type="checkbox"/>																																																
57.	Enable One-Time Entry Option	<input type="checkbox"/>																																																
58.	Enable Toggle Mode (Manual Relock)	<input type="checkbox"/>																																																
69/70	Enter Key	Enable <input type="checkbox"/> (Disable) <input type="checkbox"/>																																																



# "DL-Windows Mode" Operation / Features

This section highlights the considerations when using the ArchiTech series lock in a mode integrated with the DL-Windows software (version 5.2 and up). When using the lock in "DL-Windows Mode" (also called "Networx Mode"), credentials and lock features can be sent to the lock wirelessly using a Networx Gateway. For different types of Gateway modules, see page 4. **Note:** After lock has been configured (added) to the Networx Gateway, it will remain unlocked until a valid credential is presented to the Proximity Reader.

**IMPORTANT:** All proximity credentials manually added in "Program Card Programming" *will be deleted* upon the locks' enrollment into the DL-Windows Networx system.

If you are new to DL-Windows and Networx, stop here and read the *DL-Windows User Guide* (OI382) for a basic overview of DL-Windows. Many of the terms detailed in this manual are explained in OI382 and also the *DL-Windows for Networx User Guide* (OI383).

## Lock Types

The ArchiTech series locks are available in various design combinations, therefore the "**Lock Types**" in DL-Windows must be carefully selected. Use the control unit label (example shown at right) to make the proper selections in the DL-Windows **New Lock Profile** screen. **Note:** An identical label is located on the provided yellow Lock ID card.

N9512  
52BB6974

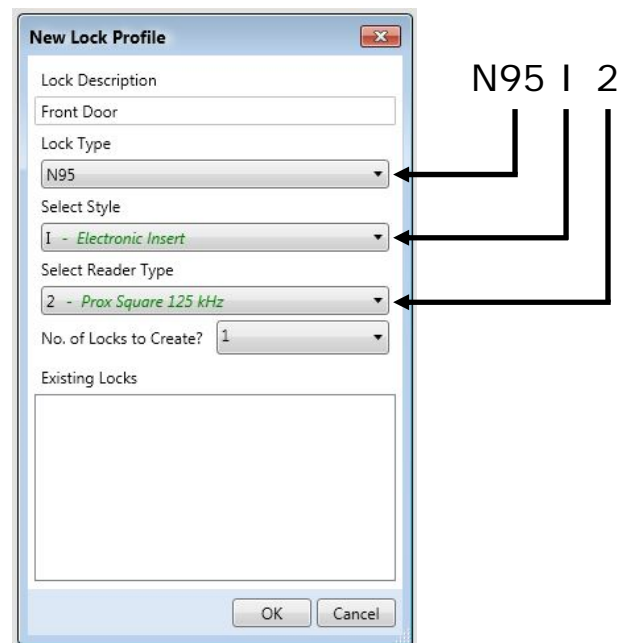
An example "**N9512**" Lock Type selection is shown below:

**Note:** Correct "Lock Types" are required for successfully linking a physical lock to the DL-Windows "Lock Profile" (see "**What is a Lock Program?**" on page 5 for further information).

## Temporary Credentials

Proximity credentials added during "Program Card Programming" are deleted upon enrollment into the DL-Windows Networx system. Even after Networx enrollment and integration, proximity credentials may still be manually added, just like in "Program Card Programming". However, upon sending a Lock Profile from DL-Windows to the lock, *all manually added cards and other credentials will be overwritten and/or deleted, with the exception of User Numbers 6000 and 6001.*

Though not recommended, if proximity credentials are manually added in "DL-Windows Mode", they will be added to the next available slot. For example, if you already added credentials to slots 12-16, the manually added credential will be written into slot 17.



## "Program Card" Considerations

- If "Program Cards" were created / enrolled ("Program Card Programming") prior to integration with DL-Windows, the "Program Cards" will NOT be overwritten and will remain in the lock memory.
- "Program Cards" are added to User Numbers ("slots") 6000 and 6001, and are logged accordingly.
- "Program Cards" have the same functionality as Administrative Users (credentials added to any of the slots numbered 2 through 11 in DL-Windows). See the "**ArchiTech User Number Definitions**" chart on page 7.

# "DL-Windows Mode" Operation / Features (cont'd)

## ArchiTech Series Features

ArchiTech series locks support most standard Networx features (e.g. Entry Delay, GP2 Toggles Passage Mode, etc.) that are available in DL-Windows. For more information regarding all of the features available with your ArchiTech series lock, see OI382 and OI383. Below are descriptions of several features and functions pertaining to the ArchiTech series models enrolled within a Networx system. **Note:** See the Glossary definition of "DEFAULT" on page 42 before proceeding.

## Functions Tab

### Program / Passage Button

By default the "Program / Passage" button is enabled, allowing for the sustained passage through the door without a credential. If you check the **Disable Passage Mode Activation** check box, the "Program / Passage" button will be disabled, thus *disallowing* sustained Passage Mode via the "Program / Passage" button. **Note:** The "Program / Passage" button's use with programming is not affected (for information about the "Program / Passage" button, see page 8).

### Hardware Selection

#### Automatic Deadbolt (No Passage Override)

The ArchiTech 9500 series (mortise) locks can be used with an "automatic" deadbolt causing the deadbolt to be extended immediately upon door closure. Because an extended deadbolt (by default) cancels Passage mode, if you wish for Passage Mode to be sustained after an automatic deadbolt extension, this **Automatic Deadbolt** checkbox must be checked.

Therefore, if **Automatic Deadbolt** is checked, Passage Mode (via an unlock Schedule or "Program / Passage" button press, etc.) will be sustained indefinitely until cancelled (via a lock Schedule or subsequent "Program / Passage" button press).

#### Enable One-Time Entry option

Used with the above-described **Automatic Deadbolt** function, the **Enable One-Time Entry option** allows for Passage Mode to be automatically canceled after the door is closed for a second time. Thus, if a door (equipped with an "automatic" deadbolt) is opened, and sustained Passage Mode is enabled via a "Program / Passage" button press, the door can be closed, re-opened (without a credential) and will lock upon a second door closure.

**IMPORTANT:** A 15 second "window of opportunity" begins after the first door closure allowing re-entry and re-exit (second door closure) without canceling sustained Passage.

**Note:** The above function is dependent on the position of the deadbolt, not the door position (Door Contact Sensor is not required for this function).

### Bluetooth

For ArchiTech series models that are equipped with Bluetooth LE technology, if you wish to disable Bluetooth connectivity for a specific Lock Profile (lock will ignore Bluetooth credentials), check the **Disable Bluetooth Connectivity** checkbox. For more information about Bluetooth connectivity, see page 33.

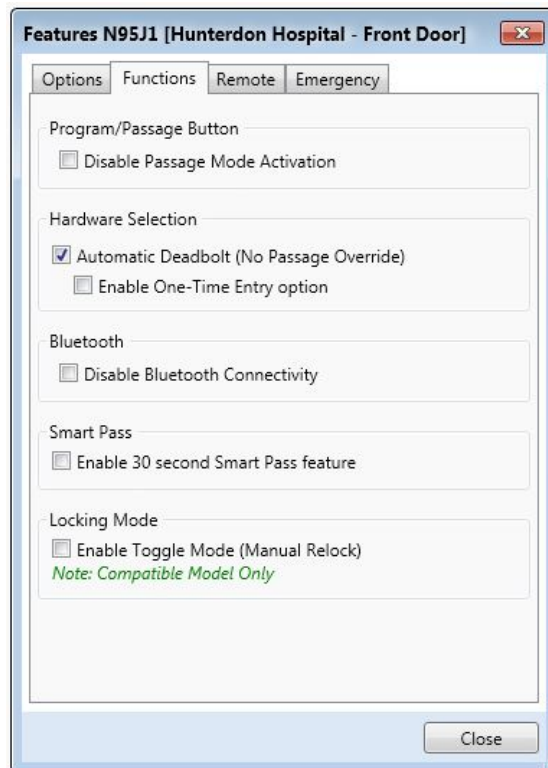
### Smart Pass

After a valid credential has been presented, the ArchiTech series lock will remain unlocked for 30 seconds OR until the door closes. Enabling this feature overrides the existing Pass Time duration. **Note:** The above function is dependent upon the door position (Door Contact Sensor required).

### Locking Mode

#### Enable Toggle Mode (Manual Relock)

See page 24, Function 67, feature 58, "Enable Toggle Mode (Manual Relock) for more information.



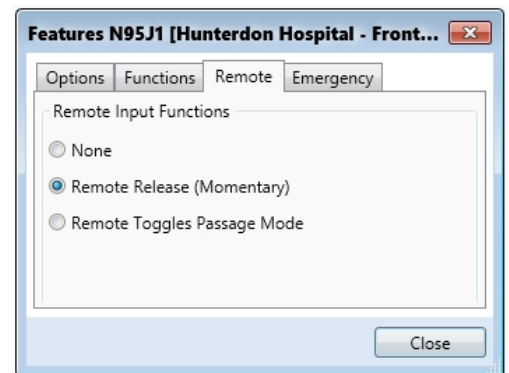
# "DL-Windows Mode" Operation / Features (cont'd)

## Remote Tab

The ArchiTech series locks allow for two programmable remote functions: **Remote Release (Momentary)** and **Remote Toggles Passage Mode**. For complete information about these DL-Windows features, see OI382 and its pages detailing the **Features** screen.

These remote release features can only be triggered by use of the RR-1BUTTON *Wireless Remote Release Button* (see WI1999) and/or the RR-4BKEYFOB *Wireless Remote Release Keyfob* (see WI2004).

**Note:** If **Remote Toggles Passage Mode** is enabled, and a Wireless Remote Release button press placed the ArchiTech series lock in an unlocked state (passage), the press and release of the "**Program / Passage**" button will take the lock out of passage (locking the lock). The opposite is also true: If a Wireless Remote Release button press placed the ArchiTech series lock in a locked state, the press and release of the "**Program / Passage**" button will place the lock in passage (unlocking the lock).



## ArchiTech Series Scheduled Events

DL-Windows software allows you to create **Schedules** containing "Events". ArchiTech series locks support all standard scheduled Events such as **Unlock**, **Disable Group**, **Enable User**, etc., with two additional Events, **Power Saving Mode** and **Bluetooth ON/OFF**. For more information regarding all of the scheduled Events available, creating Time Zones and Events in the DL-Windows **Schedule** Screen, refer to OI382 and OI383.

### Power Saving Mode ON / OFF

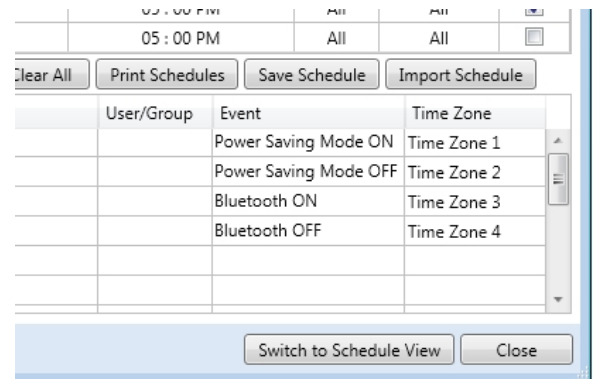
The ArchiTech series locks can be placed into a **Power Saving Mode** for specified periods of time. By creating **Power Saving Mode** Events, the lifespan of the batteries can be greatly increased.

For example, if the ArchiTech series lock is installed inside a business office where the office closes and remains empty at night, a Schedule can be created to place the ArchiTech series lock into a Power Saving Mode, from 5:05 PM through 9:00 AM every weekday.

Schedules for weekends and holidays can also be created to suit the specific circumstances of the installation, maximizing battery life even further.

**IMPORTANT:** During Power Saving Mode, proximity credentials WILL function normally, **but because the internal radio is off, ALL communications, including Wireless Remote Releases, will NOT function.**

To place the ArchiTech series lock into a Power Saving Mode via a Schedule, select "**Power Saving Mode On**" in the **Event** column located in the **Schedule Entry** area. See image at right for an example "**Power Saving Mode On**" selection.



### Bluetooth ON / OFF

For ArchiTech series models that support Bluetooth, the internal Bluetooth radio can be toggled on and off, as desired. Turning the Bluetooth radio off will deny access to Bluetooth Users and will also increase the lifespan of the batteries.

For example, if the ArchiTech series lock is installed inside a business office where the office closes and Bluetooth Users should be denied access, a Schedule can be created to turn off the Bluetooth radio from 5:05 PM through 9:00 AM every weekday, thus ignoring all Bluetooth credentials.

To disable Bluetooth in an ArchiTech series lock via a Schedule, select "**Bluetooth OFF**" in the **Event** column located in the **Schedule Entry** area. See the accompanying image for an example "**Bluetooth ON / OFF**" selection.

**TIP:** Like all scheduled Events, **Power Saving Mode** or **Bluetooth ON / OFF** may be programmed to coincide with other Schedules. For example, the lock can lock every day at 5:00 PM and also begin Power Saving Mode at 5:00 PM.

# Emergency Commands

## Overview

The ArchiTech series locks can be programmed to send and/or respond to Emergency Commands ("Emergency Lock Down", "Emergency Passage" and "Return to Normal"). Emergency Commands can be initiated an RR-4BKEYFOB *Wireless Remote Release* or initiated from the Network server running DL-Windows. (**Note:** "Emergency Passage" is not available with the *Wireless Remote Release*). Emergency Commands are available in two types: "Global" or "Local".

- With "Global Emergency Commands", activating the Emergency Command changes the state of all locks in the entire system.
- With "Local Emergency Commands", only the lock that initiates the Emergency Command will change state; activating the Emergency Command does NOT change the state of all locks in the entire system.

For more information about how Emergency Commands work with your ENTIRE system, see the *DL-Windows for Network User's Guide* (OI383).

## Understanding "Global" vs. "Local"

The following features should be understood before using **Emergency Commands** with your ArchiTech series lock. Below describes the various features available for **Global Emergency Commands** or **Local Emergency Commands**, or combinations of both.

**TIP:** If using an RR-4BKEYFOB *Wireless Remote Release*, before reading this page, we recommend that you read the documentation that came with it, and also the "Wireless Remote Releases" section on page 36.

### Receiving Emergency Commands

#### Lock Responds to Global Emergency Commands

- **When enabled:** The lock **WILL** accept and adhere to Emergency Commands that disseminate from another lock or from DL-Windows. **Note:** This feature does not need to be enabled (checked) for the lock to accept commands from an RR-4BKEYFOB *Wireless Remote Release*.
- **When disabled:** The lock **WILL NOT** accept nor adhere to Emergency Commands that disseminate from another lock or from DL-Windows. **CAUTION:** *Disabling (un-checking) this feature could be of great consequence for the safe administration of your Network system.*

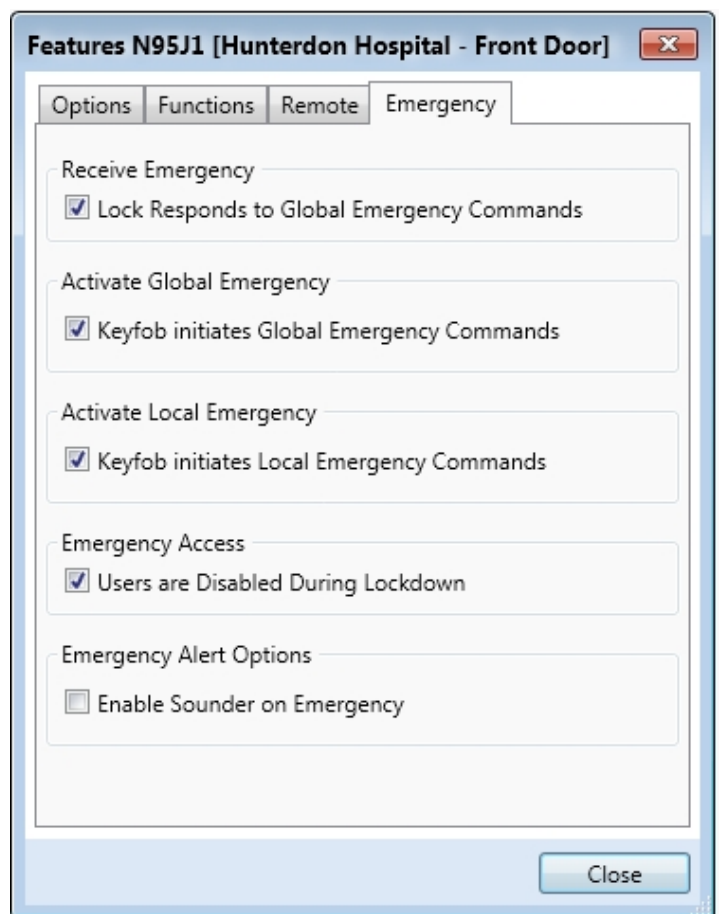
### Activating Global Emergency Commands

**Keyfob initiates Global Emergency Commands:** When enabled (checked), if an Emergency Command is initiated from an RR-4BKEYFOB *Wireless Remote Release*, the "paired" lock will first inform the Gateway to broadcast the Emergency Command to all locks assigned to the same "**Gateway Group**", **then** the paired lock will respond to that Emergency Command accordingly (if the above "**Lock Responds to Global Emergency Commands**" is enabled).

**Note:** See OI383 for more information about Gateway Emergency Groups.

### Activating Local Emergency Commands

**Keyfob initiates Local Emergency Commands:** When enabled (checked), if an Emergency Command is initiated from an RR-4BKEYFOB *Wireless Remote Release*, the paired lock will immediately change state accord-



# Emergency Commands (cont'd)

ingly. The Emergency Command will NOT be sent to the Gateway and therefore will NOT be sent to other locks in the system.

**TIP: Combining Global and Local Features:** You can combine the various Global and Local Emergency features to customize your system.

**Example #1:** DL-Windows by default enables (checks) all of the features, as shown above in the **Features** dialog. What will happen when all features are enabled and an "**Emergency Lock Down**" command is initiated from a keyfob? Because the **Activate Local Emergency** commands are enabled, the lock that receives and initiates the Emergency Command will lock down, then the lock will inform the Gateway to broadcast the Emergency Command to all locks assigned to the same "**Gateway Group**".

**Example #2:** This example is known as the "pull station option", where the **Activate Global Emergency** command is checked, the **Activating Local Emergency** command is not checked, and the "**Lock Responds to Global Emergency Commands**" is unchecked. If an "**Emergency Lock Down**" command is then initiated, the lock will first inform the Gateway to broadcast the Emergency Command to all locks assigned to the same "**Gateway Group**", then the lock will ignore the broadcast when received.

## Emergency Users

### Activating Emergency Commands

By default, Administrative Users (Users 1 through 11) automatically have the ability to initiate Emergency Commands from the keypad. In addition, "Basic Users" (Users 12+) may be granted the ability to initiate Emergency Commands from the keypad by adding them as Emergency Users in DL-Windows (for more information about adding Emergency Users in DL-Windows, see OI383). **Note:** All paired Wireless Remote Releases have the ability to initiate Emergency Commands (see page 36 for more information).

When a User Code from an Administrative or Emergency User is pressed at any lock keypad, first the lock unlocks, then the lock permits the use of the following Emergency Commands:

[ _ _ _ _ ]	...press <span style="border: 1px solid black; padding: 2px;">9</span> <span style="border: 1px solid black; padding: 2px;">1</span> <span style="border: 1px solid black; padding: 2px;">1</span> to issue " <b>Emergency Lock Down</b> "
Administrative or Emergency User Code	...press <span style="border: 1px solid black; padding: 2px;">0</span> <span style="border: 1px solid black; padding: 2px;">0</span> <span style="border: 1px solid black; padding: 2px;">0</span> to issue " <b>Emergency Passage</b> "
	...press <span style="border: 1px solid black; padding: 2px;">1</span> <span style="border: 1px solid black; padding: 2px;">2</span> <span style="border: 1px solid black; padding: 2px;">3</span> to issue " <b>Return to Normal</b> "

### Access During an Emergency

- **When enabled:** If the feature **Users are Disabled During Lockdown** is enabled (checked) for a specific lock, and when the Networx system is in an Emergency Lock Down state, "Basic Users" (Users 12+) are denied the ability to unlock the physical lock (credentials for these Basic Users are ignored). The proximity credentials added as Administrative Users (Users 2 through 11), "Program Cards", Bluetooth credentials, as well as all "Emergency Users" **remain enabled**, retaining the ability to unlock a secured lock.
- **When disabled:** If the feature **Users are Disabled During Lockdown** is disabled (unchecked) for a specific lock, and when the Networx system is in an Emergency Lock Down state, ANY valid credential that exists in the lock's internal memory will be allowed to unlock the secured lock, regardless of User Number.

## Emergency Alert Options

### Sounder

If **Enable Sounder on Emergency** is enabled (checked), upon receiving an Emergency Command, the integral sounder will beep once per second for 30 seconds.

**Tip:** Only "Local" Emergency Commands are supported when using an **AL-IME-USB** Gateway . See page 4 for Gateway model descriptions.



## Overview

The J and T "style" ArchiTech series locks contain Bluetooth LE technology that allows for entry via a smartphone application ("app"). The iLock smartphone app works essentially as any other type of proximity credential; simply launch the iLock app and tap the **Unlock** button to allow entry. For added security, an optional password can be set in the iLock app that would then be required for every unlock request. **Note:** Up to 27 Bluetooth Users are supported for any one ArchiTech series lock.

## Downloading the iLock App

- **For iPhone Users:** Go to your iTunes store, search for "iLock" and download the app.
- **For Android Users:** Go to your Google Play store, search for "iLock" and download the app.

**Note:** The following special permissions are required:

- Device Location
- File Access.

## Enrolling Bluetooth Credentials

After the iLock app has been downloaded and installed on your smartphone:

1. Run the iLock app and the **Settings** screen opens.
2. Place the ArchiTech series lock into Enroll Mode by pressing the "**Program / Passage**" button once (Enroll Mode = continuous beeping with green LED flashes).

Depending on the programming "environment" of the lock (see page 9), Enroll Mode is entered as follows:

- **Initial lock startup:** Simply press the "**Program / Passage**" button once
- **Program Card Programming:** Present a "Program Card" *and with the state of the lock "unlocked"*, press the "**Program / Passage**" button once
- **DL-Windows Mode:** Present a "Program Card" OR any Administrative User (2-11); *with the state of the lock "unlocked"*, press "**Program / Passage**" button once

3. Within 30 seconds, tap "**Add a New Lock**" on the iLock app.
4. In the **Select Lock** screen, select the lock that displays the device name of "**MyLock**". Lock acknowledges with two beeps.
5. Within 120 seconds, enter a **Lock Name** and password (maximum 20 alphanumeric characters).
  - **Successful Pairing:** Lock sounds 4 beeps with 4 green LED flashes
  - **Unsuccessful Pairing:** Lock sounds 7 beeps with 7 red LED flashes.
6. **Exit Enroll Mode:** Press and firmly hold the "**Program / Passage**" button for 4 seconds until you hear a series of beeps.

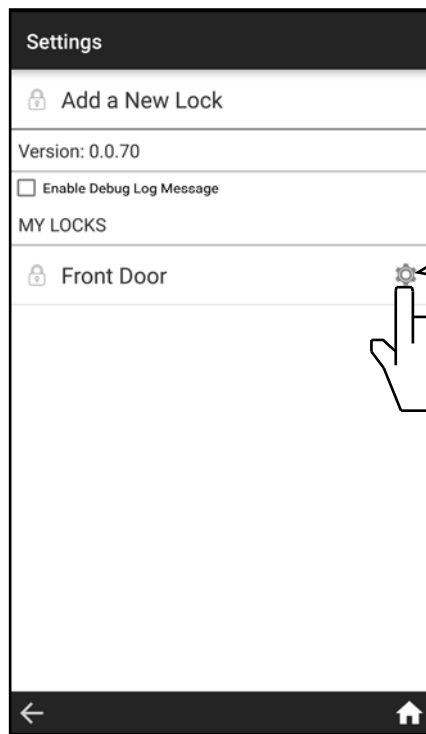
Follow the above steps for each additional Bluetooth credential.

## Bluetooth Credential Considerations

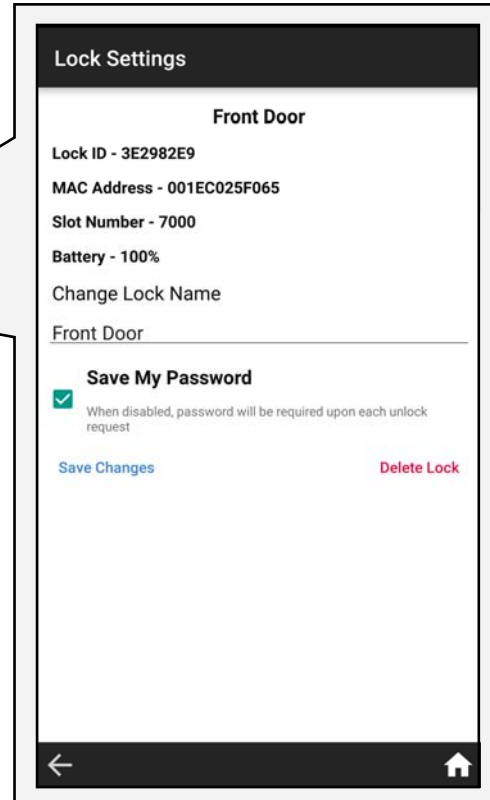
- If Bluetooth credentials were created / enrolled using "Program Card Programming" prior to integration with DL-Windows, the Bluetooth credentials will NOT be overwritten and will remain in the lock memory.
- Bluetooth credentials are added to slots 7000 through 7089\*, and are logged accordingly.
- The first two Bluetooth credentials added (slots 7000, 7001) have the same functionality as Administrative Users (credentials added to any of the slots numbered 2 through 11 in DL-Windows). Therefore, the first two Bluetooth Users have the ability to add additional Bluetooth credentials. See the "**ArchiTech User Number Definitions**" chart on page 7.

\*The latest firmware has an expanded Bluetooth capacity, with credentials added to slots 7000 through 7089. Please note that this high number, which indicates the maximum number of Bluetooth users, will vary depending on the firmware installed.

# Using the iLock App



iLock App: "Settings" screen



iLock App: "Lock Settings" screen (see below)

## Lock Settings

### Lock ID

(Lock Serial Number): Displays the physical lock's unique serial number assigned and programmed into the lock firmware at the factory. Network locks are identified in DL-Windows by this unique serial number.

### MAC Address:

Displays the unique 12-digit MAC address of the Bluetooth radio module of the selected lock.

### Slot Number

Used interchangeably with *User Number*, this number represents the location within the lock's internal programming memory. The location and therefore the Slot Number determines the abilities of that User. The first two Bluetooth Users are always added to slots 7000 and 7001 respectively; these Users have Administrative rights. All subsequently added Bluetooth Users (7002 - 7026) are "Basic" Users. For more information about ArchiTech User Number Definitions, see page 7.

### Battery

Indicates the latest percentage of remaining usable capacity of the battery in the selected lock, (updated upon each successful communication). **Important:** The percentage will equal zero upon a Low Battery Warning indication (see page 37 and 40), therefore 50% represents halfway to a Low Battery state .

## Change Lock Name

Displays existing Lock Name created in step 5 in "Enrolling Bluetooth Credentials" above. Upon selection, smartphone keyboard will appear allowing changes. **Note:** Tap "**Save Changes**" to retain all edits.

## "Save My Password" Feature

Checked (enabled) by default, password created in step 5 in "Enrolling Bluetooth Credentials" above is not required for each unlock request. When unchecked (disabled), each time the Unlock Button is selected from the home screen a prompt will appear to enter your password.

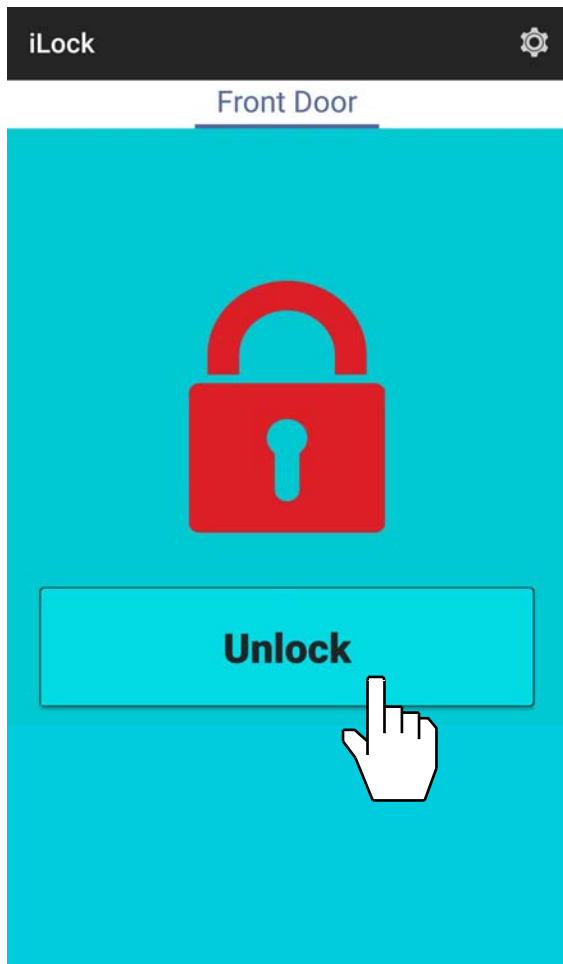
## Save Changes

Retains changes to the Lock Name or the "Save My Password" Feature.

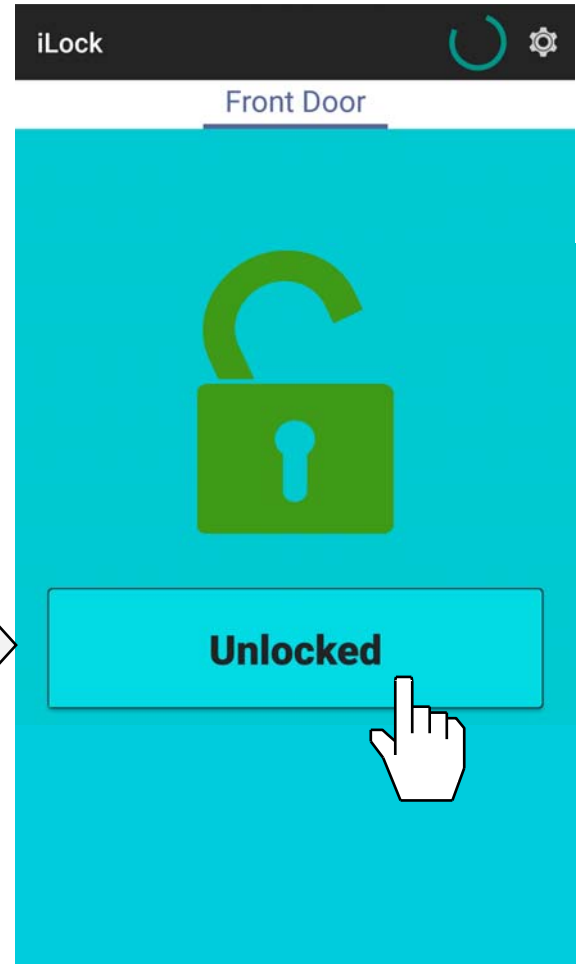
## Delete Lock

Removes the selected Network lock from the iLock app.

## Using the iLock App (cont'd)



Press **Unlock** to send an unlock request to the selected ArchiTech series lock. The lock will unlock within a few seconds (this time varies with smartphone models).



Red padlock turns green upon unlock (and remains green / unlocked for the duration of the programmed Pass Time).

See Function 67, feature 58, "**Enable Toggle Mode (Manual Relock)**" on page 24 for more information.

# Wireless Remote Releases

Two types of "Wireless Remote Release" devices are compatible with the ArchiTech series door locks: The RR-1BUTTON *Wireless Remote Release Button* (see WI1999) and RR-4BKEYFOB *Wireless Remote Release Keyfob* (see WI2004). Whether the Wireless Remote Release contains a single button (RR-1BUTTON) or four buttons (RR-4BKEYFOB), each button can be "paired" (connected) with one ArchiTech series lock. This means, for example, the four buttons on the RR-4BKEYFOB can each be paired with four separate ArchiTech series locks. In addition, each individual ArchiTech series lock contains ten (10) "slots" ("User Numbers"), and each "slot" is available to accommodate one paired Wireless Remote Release button. Therefore, each individual ArchiTech series lock can ultimately be paired with up to ten Wireless Remote Release buttons on multiple Wireless Remote Release devices.

**Note:** Since each button can ONLY be paired with one specific Networkx-integrated ArchiTech series lock at a time, when a previously paired button is later paired with a second locking device, the first pairing is erased.

Before you "pair" (connect) your Wireless Remote Release buttons, here are some important things to consider:

- Though Wireless Remote Releases can be enrolled when the lock is in "Program Card Programming", migration to "DL-Windows Mode" after Wireless Remote Releases are enrolled requires that the lock be defaulted and re-initialized (page 38), *clearing all previously programmed Users and/or paired Wireless Remote Releases*.
- If your lock has been placed into a Power Saving Mode via a DL-Windows Schedule, Wireless Remote Releases will **NOT** function.

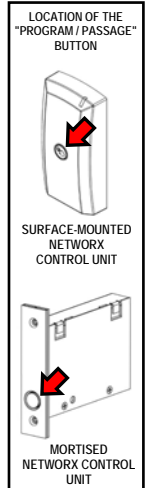
## Pairing Wireless Remote Release Buttons

Before you begin, note that the pairing steps below must all be performed within thirty (30) seconds. Ten of the thirty seconds are used during step 3, leaving little time for error or delays. Therefore, before proceeding, *read through the steps first* to become familiar with this simple procedure.

1. Select a Wireless Remote Release "button" you wish to pair. Selecting a button in advance will greatly assist this process. Keep the Wireless Remote Release ***in your hand*** as you perform the next steps.
2. Place the ArchiTech series lock into Enroll Mode by pressing the "**Program / Passage**" button once (Enroll Mode = continuous beeping with green LED flashes). The 30 second timeout begins now.

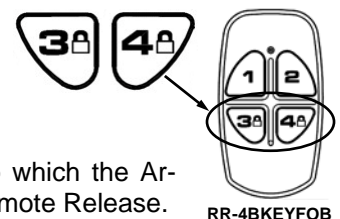
Depending on the programming "environment" of the lock (see page 9), Enroll Mode is entered as follows:

- **Initial lock startup:** Simply press the "**Program / Passage**" button once
  - **Program Card Programming:** Present a "Program Card" and with the door open, press the "**Program / Passage**" button once
  - **DL-Windows Mode:** Present a "Program Card" OR any Administrative User (2-11); with the door open, press "**Program / Passage**" button once
3. Immediately ***press and hold*** the Remote Release button and observe the Remote Release LED:
    - a. The red LED lights...keep holding the button...
    - b. The LED flashes green, release the button...
    - c. Wait and observe the LED as follows:
      - LED solid green = Pairing successful (also a double-beep and green LED on the Proximity Reader)
      - LED solid red = Pairing unsuccessful, start again at step 1.
  4. **Exit Enroll Mode:** Press and firmly hold the "**Program / Passage**" button for 4 seconds until you hear a series of beeps.



## Emergency Lock Down (via Wireless Remote Release)

The ArchiTech series locks have the added ability to accept Emergency Lock Down commands from a Wireless Remote Release (model RR-4BKEYFOB only). When buttons 3 and 4 are pressed simultaneously, within seconds an Emergency Lock Down command is sent to all locks to which the RR-4BKEYFOB is currently paired (up to 4). Conversely, pressing buttons 1 and 2 simultaneously will send a Return to Normal command, returning the paired locks back to the state they were in prior to receiving the Emergency Lock Down command. See page 31 for the two different modes (**Understanding "Global" vs. "Local"**) to which the ArchiTech series locks respond when an Emergency Command when sent from a Wireless Remote Release.



# Low Battery and Battery Replacement

## Low Battery Warning

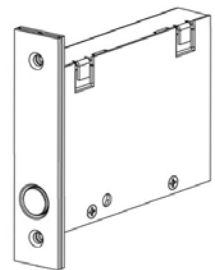
When a valid proximity credential is presented to the lock and the batteries are weak, a steady tone will sound for the duration of the Pass Time ("Pass Time" is the duration the lock remains unlocked after access is granted). Discard the weak batteries and replace with four (4) AA-size 1.5 volt alkaline batteries. Always replace weak batteries as soon as possible.

## Battery Replacement

The batteries are located within the **Control Unit** (each type pictured below), therefore the battery replacement steps will vary with the design. Avoid pressing the "**Program / Passage**" button during this procedure (see diagrams on page 8).

To replace batteries in the **Mortised Networkx Control Unit**:

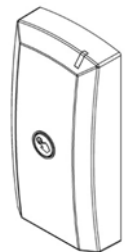
1. Remove the two 8-32 x 1/4" Phillips Flat-Head screws that secure the flush **Finishing Plate** that covers the **Mortised Networkx Control Unit**. Put screws aside in a safe place.
2. The **Finishing Plate** is connected to the internal PC board with a wire (take note of how the wire was placed under the PC board at the factory). Gently lift and move the **Finishing Plate** to the side.
3. Pull out the battery connector wires and disconnect the plugs.
4. Taking note of its original orientation, pull out the battery pack.
5. Remove the screw securing the battery pack top cover, then lift the top cover. Remove all weak batteries and replace with fresh batteries, observing polarity. NEVER mix weak batteries with fresh batteries.
6. Replace the battery pack top cover and secure with the screw. Insert the battery pack in the same orientation as its removal in step 4.
7. Connect the battery connector plug. If you **do not** hear 3 beeps when power is re-applied, all programming and settings have been retained, and the lock will be ready for use. If you **do** hear 3 beeps when power is re-applied, wait 15 seconds for the LED to flash red 7 times and 7 beeps will sound (the clock will need to be reset using DL-Windows).
8. Gently push the battery wires (and any other loose wires) back into the **Control Unit**.
9. Return the **Finishing Plate** to its original location and secure with the two 8-32 x 1/4" Phillips Flat-Head screws.



MORTISED  
NETWORKX CONTROL  
UNIT

To replace batteries in the **Surface-Mounted Networkx Control Unit**:

1. Using the supplied Allen key, remove the mounting screw (#6-32 Allen Head countersunk U-cut Dog Point screw, part #SC681, shown at right). Put screw aside in a safe place.
2. Lift the bottom of the **Surface-Mounted Networkx Control Unit** and unhook the top. Gently lift from the door surface; do not pull wires. It is OK to let the unit "hang" from the door.
3. With two fingers, firmly grasp the battery wires connected to the white plug. Pull the wires until the plug releases from the white female socket. It is OK to use some force in this step. **Do not remove the battery pack yet.**
4. Taking note of its original orientation (top cover screws facing "down"), remove the battery pack.
5. Remove both screws securing the battery pack top cover, then lift the top cover. Remove all weak batteries and replace with fresh batteries, observing polarity. NEVER mix weak batteries with fresh batteries.
6. Replace the battery pack top cover and secure with two screws. Insert the battery pack in the same orientation as its removal in step 5.
7. Insert the white battery plug into the white socket and press firmly until secure. If you **do not** hear 3 beeps when power is re-applied, all programming and settings have been retained, and the lock will be ready for use. If you **do** hear 3 beeps when power is re-applied, wait 15 seconds for the LED to flash red 7 times and 7 beeps will sound (the clock will need to be reset using DL-Windows).
8. Ensure all wires are pushed back into the door to avoid pinching wires. Carefully hook the top of the **Surface-Mounted Networkx Control Unit** into the top of the **Control Unit Mounting Plate** (see installation instructions if necessary) and press the bottom until flush with the door surface. Replace the #6-32 Allen Head countersunk U-cut Dog Point screw (part #SC681 as shown above) at the bottom of the **Surface-Mounted Networkx Control Unit** and tighten securely. Replace all hardware removed as required.



SURFACE-MOUNTED  
NETWORKX  
CONTROL UNIT

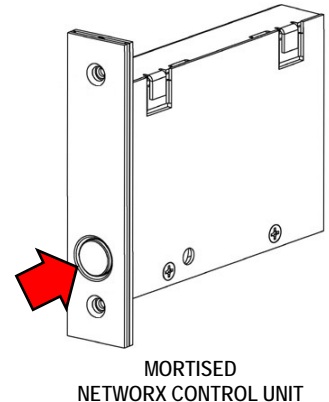
# Erase All Programming

## Erase All Programming (Restore the "out of box" factory condition)

To return the ArchiTech series lock to its original condition, when the lock and all components were first removed from their factory packaging, proceed as follows for the specific model type in your installation:

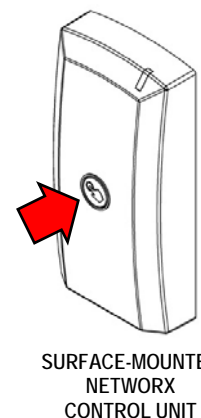
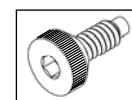
To erase all programming in the **Mortised Networkx Control Unit**:

1. Remove the two 8-32 x 1/4" Phillips Flat-Head screws that secure the flush **Finishing Plate** that covers the **Mortised Networkx Control Unit**. Put screws aside in a safe place.
2. The **Finishing Plate** is connected to the internal PC board with a wire (take note of how the wire is placed under the PC board at the factory). Gently lift and move the **Finishing Plate** to the side.
3. Pull out the battery connector wires and disconnect the plugs.
4. Press and hold the "**Program / Passage**" button (see arrow in image at right) for 15 seconds, then release.
5. Reconnect the battery connector plug. Listen for 3 beeps. Press and firmly hold the "**Program / Passage**" button again until you hear multiple beeps, then release the button. The lock will continue to beep and flash the red LED while residual programmed data clears and the lock initializes. A final 2 beep/green flash sequence will occur, indicating successful completion of the power up procedure. **Note:** This step can take up to 15 seconds.
6. Gently push the battery wires (and any other loose wires) back into the **Control Unit**.
7. Return the **Finishing Plate** to its original location and secure with the two 8-32 x 1/4" Phillips Flat-Head screws.



To erase all programming in the **Surface-Mounted Networkx Control Unit**:

1. Using the supplied Allen key, remove the mounting screw located in the previous step (#6-32 Allen Head countersunk U-cut Dog Point screw, part #SC681, shown at right). Put screw aside in a safe place.
2. Lift the bottom of the **Surface-Mounted Networkx Control Unit** and unhook the top. Gently lift from the door surface; do not pull wires. It is OK to let the unit "hang" from the door.
3. With two fingers, firmly grasp the battery wires connected to the white plug. Pull the wires until the plug releases from the white female socket. It is OK to use some force in this step.
4. Press and hold the "**Program / Passage**" button (see arrow in image at right) for 15 seconds, then release.
5. Re-insert the white battery plug into the white socket and press firmly until secure. Listen for 3 beeps. Press and firmly hold the "**Program / Passage**" button again until you hear multiple beeps, then release the button. The lock will continue to beep and flash the red LED while residual programmed data clears and the lock initializes. A final 2 beep/green flash sequence will occur, indicating successful completion of the power up procedure. **Note:** This step can take up to 15 seconds.
6. Ensure all wires are pushed back into the door to avoid pinching wires. Carefully hook the top of the **Surface-Mounted Networkx Control Unit** into the top of the **Control Unit Mounting Plate** (see installation instructions if necessary) and press the bottom until flush with the door surface. Replace the #6-32 Allen Head countersunk U-cut Dog Point screw (part #SC681 as shown above) at the bottom of the **Surface-Mounted Networkx Control Unit** and tighten securely. Replace all hardware removed as required.



# Power Down -- Retain Existing Programming

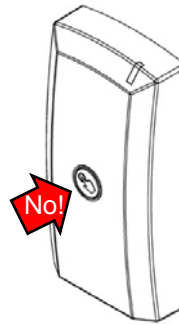
## Power Down--Retain Existing Programming

Use when re-applying power to a lock already in use (you wish to retain the Lock Program), such as when moving an existing lock to a new door or changing the batteries. In this case, the lock is to be dismantled and powered down for an extended period.

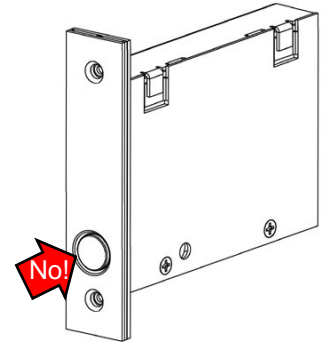
Follow all the steps for "**Low Battery and Battery Replacement**" on page 37 for the Control Unit installed, however **DO NOT** touch the "**Program / Passage**" button **AT ANY TIME** during the procedure.

If the lock is powered down for an extended period of time, and if you **do not** hear 3 beeps when power is re-applied, all programming and settings have been retained, and the lock will be ready for use.

If you **do** hear 3 beeps when power is re-applied, wait 15 seconds for the LED to flash red 7 times and 7 beeps will sound (the clock will need to be reset using DL-Windows).



SURFACE-MOUNTED  
NETWORK  
CONTROL UNIT



MORTISED  
NETWORK CONTROL UNIT

## LED and Sounder Indications

With a fully charged battery, the LED and sounder provide visual and audible feedback. The LED on the **Surface-Mounted Network Control Unit** mimics the LED located on the **Proximity Reader**.

ACTIVITY	LED FLASHES	SOUNDER BEEP(S)	COMMENTS
Access Granted / Wireless Remote Release button press	2 Green	2	Lock unlocks for duration of Pass Time ("Pass Time" is the duration the lock remains unlocked after access is granted).
Invalid Credential	7 Red	7	Invalid proximity credential presented that does not exist in the Lock Program memory.
<b>"Program / Passage"</b> button press (while door is open)	2 Green	2	Passage mode toggled.
Successful Credential Enrollment (Valid Read)	2 Green	2	Proximity credential added to Lock Program memory successfully.
Unsuccessful Credential Enrollment (Invalid Read)	7 Red	7	Proximity credential enrollment denied (Lock Program memory full, credential already exists, credential not fully read by Proximity Reader, etc.).
Enter Enroll Mode	1 Red, 2 Green	10	Sounder cadence shorter for entering Enroll Mode compared with exiting.
Exit Enroll Mode	1 Red, 2 Green	10	This red LED and sounder combination denotes a "Successful" Enroll Mode exit. Sounder cadence longer for exiting Enroll Mode compared with entering.
Waiting for credential (in Enroll Mode)	Rapid Green for 25 seconds, then Red for final 5 seconds	Rapid beeps for entire 30 second duration	Automatically times out after 30 seconds total.
Valid but Disabled Credential	1 Green, 4 Red	1 long, 5 short	Credential exists in Lock Program memory, but is disabled.
Emergency Commands are in effect	1 Red every two seconds	--	See page 31-32; also see OI382 and OI383 for more information.
Low Battery Warning	Red LED and sounder steady during Pass Time		("Pass Time" is the duration the lock remains unlocked after access is granted). See page 37 before changing batteries.
"DL-Windows Mode" Re-activated	2 Green	2	Manually enabled "DL-Windows Mode".
Door Ajar Sounder	Red flash and beep every second for 25 seconds		Occurs after Door Ajar Trip Time expires. "Sounder on Door Ajar" feature must be programmed. See page 8, " <b>Door Contact Sensor</b> ".





# Glossary

**ACCESS** = Entry into a restricted area.

**ADMINISTRATIVE USERS** = Credential data added to any of the slots ("User Numbers") numbered 2 through 11). See... **USERS 2-11**.

**AUDIT TRAIL** = A date/time stamped log of previous lock events.

**BASIC USERS** = Credential data assigned to User Numbers 12-5000 are "Basic Users". These Users possess no programming abilities, nor Administrative abilities.

**BLUETOOTH** = The standard WPAN ("Wireless Personal Area Network") for transmitting short-range digital data via radio waves.

**BLUETOOTH CREDENTIAL** = A Bluetooth enabled device acts as a traditional type of proximity design.

**BLUETOOTH USER** = A person who has been provided with a Bluetooth credential for access through the door.

## CLOCK

- **REAL TIME CLOCK** = An accurate built-in clock that allows date/time stamping of events. The clock can be slowed or speeded up to fine tune long term accuracy to within three minutes per year. Programmed only through DL-Windows.

- **CLOCK SETTINGS** = Printout includes date, time, weekday, and clock speed.

**CREDENTIAL** = A generic word used to indicate a proximity card, a proximity "fob", a Bluetooth credential or other types of proximity designs.

**CONFIGURE** = In the DL-Windows software, the word "configure" means to "assign" a discovered physical ArchiTech series lock to a Gateway module, thus ensuring a fixed wireless communication channel exists between a selected physical lock and a selected Gateway.

**DATE** = Month, Day and Year entered as MMDDYY. Programmed only through DL-Windows.

**DAY OF WEEK** = Sunday through Saturday (where 1 = Sunday and 7 = Saturday). Programmed only through DL-Windows.

**DEFAULT** = The original settings that were set at the factory. In other words, it is the device's (such as a lock) original factory condition when the device was first taken out of its box. With

an ArchiTech lock, its default settings are permanently encoded within the lock's fixed memory, and when the lock is first started, or when power is removed and re-applied (see page 39), the original factory default settings are re-loaded and take effect.

**DISABLE** = Turn off.

**"DL-WINDOWS MODE" RE-ACTIVATION** = Procedure that re-allows the ArchiTech series door lock to be available for discovery by a Networx Gateway and by DL-Windows. Once discovered and enrolled into a Networx system, all programming can be performed through the Networx DL-Windows software (v5.2 or later).

**DOWNLOAD** = Send data to lock.

**EMERGENCY GROUP** = Upon the addition of each Gateway into an Account, the Gateway is automatically placed into an Emergency Group ("**GROUP A**" by default). This is done so that upon the initiation of an Emergency Command, ALL Gateways in the Emergency Group (and their assigned locks) will respond to Emergency Commands issued from DL-Windows. In addition, the automatic placement of a new Gateway into an Emergency Group allows for keypad-initiated Emergency Commands to lock down an entire system from a single wireless lock. See OI383 for more information.

**ENABLE** = Turn on.

**EVENTS** = Recorded lock activity.

**FORCED DOOR DETECTION** = If this DL-Windows feature is enabled, sounder will trigger upon "door open" without prior valid credential entry. Not available for all lock models.

**Note:** For use with door position contacts.

**GATEWAY GROUP** = See...**EMERGENCY GROUP**

## GROUP

- **USER GROUP** = Defining a User to specific Groups allows User entry when the Group is allowed entry. Programmed only through DL-Windows.

- **ONE TIME ONLY FOR GROUP 3 USERS** = If selected in DL-Windows, allows Group 3 proximity credential to unlock the lock one time only (thereafter their proximity credential becomes disabled). See OI382.

**GUARD TOUR** = Associated with User 298 and

## Glossary (cont'd)

User 299. A Guard Tour proximity credential is used to log the movement of a security guard as he or she makes rounds from one assigned guard tour station to the next. Presenting the User 299 proximity credential provides precise verification and accountability of a guard's movement by logging the location with a time and date stamp in the Event Log ("Audit Trail"). **Note:** Proximity credentials assigned to User 298 and User 299 are **not** access credentials (meaning these credentials do NOT allow the security guard to pass through the secured door).

**iLock** = Android or iOS smartphone Bluetooth LE application ("app") that allows for manual remote unlock of Alarm Lock ArchiTech series devices (where equipped).

**LOG** = See... **AUDIT TRAIL**.

**PASSAGE** = Allow anyone to pass through the door without a credential ("door is unlocked" and "lock is an unlocked state"). See... **CREDENTIAL**.

**PAIR** = To connect a button (located on the RR-1BUTTON *Wireless Remote Release Button* or the RR-4BKEYFOB *Wireless Remote Release Keyfob*) with an ArchiTech series locking device for the purpose of locking or unlocking the lock, or initiating Emergency Commands. Each button on the *Wireless Remote Release* can be "paired" (connected) with one ArchiTech series locking device (four buttons on the RR-4BKEYFOB can be paired with four separate locking devices).

**PASS TIME** = The duration in seconds that the physical lock will remain unlocked after a valid credential has been presented.

**POWER SAVING MODE** = To maximize battery life, DL-Windows allows for the creation of **Schedules** containing a "**Power Saving Mode On**" Event that places the ArchiTech series lock into low power operation for specified periods of time.

**PROGRAM CARDS** = Used with "Program Card Programming" operation, two ordinary proximity cards are made into "Program Cards", permitting all programming to be performed at the lock's Proximity Reader. The data for these two "Program Cards" are placed into slots 6000 and 6001. For a comprehensive understand-

ing, see the "**ArchiTech User Number Definitions**" table on page 7 and '**Select "Program Card Programming" Operation**' on page 11.

**REMOTE INPUT** = Allows entry into a restricted area by pressing a button connected to the two REMOTE INPUT wires (two internal white wires) by someone on the protected side of the door.

**RX REQUEST TO EXIT** = See... **FORCED DOOR DETECTION**.

**SCHEDULE** = A programmed operation (enable/disable, lock/unlock, etc.) on a specific day (Sunday through Saturday) and time. Programmed only through DL-Windows.

**SCHEDULES, QUICK** = Any one of four most common types of Schedules can be programmed. Programmed only through DL-Windows.

**TIME** = Hours and Minutes in the HHMM format. Programmed only through DL-Windows.

**TIME / DATE STAMP** = A recorded date and time that an event occurred.

**TIMEOUT** = Allowing or restricting operation for a specified duration.

**UPLOAD** = Receive data from the lock.

**USER** = A person who has been provided with a proximity credential for access through the door.

**USER LOCKOUT, TOTAL** = All Users to be locked out and thus denied access. Proximity credentials will not unlock the lock.

**USERS 2-11** = Credential data assigned to User Numbers 2-11 are "Administrative Users". These Users possess added abilities, including programming abilities (able to place lock into Enroll Mode and to enroll additional Basic User credentials or a Wireless Remote Release). These Users are also "Emergency Users" (during an Emergency state, their credential can unlock the physical lock for the duration of the Pass Time). See the chart on page 7 for details.

# ArchiTech Networx Limited Warranty

NAPCO Security Technologies, Inc. (NAPCO) warrants its products to be free from manufacturing defects in materials and workmanship for twenty four months following the date of manufacture. NAPCO will, within said period, at its option, repair or replace any product failing to operate correctly without charge to the original purchaser or user.

This warranty shall not apply to any equipment, or any part thereof, which has been repaired by others, improperly installed, improperly used, abused, altered, damaged, subjected to acts of God, or on which any serial numbers have been altered, defaced or removed. Seller will not be responsible for any dismantling or reinstallation charges, environmental wear and tear, normal maintenance expenses, or shipping and freight expenses required to return products to NAPCO. Additionally, this warranty shall not cover scratches, abrasions or deterioration due to the use of paints, solvents or other chemicals.

THERE ARE NO WARRANTIES, EXPRESS OR IMPLIED, WHICH EXTEND BEYOND THE DESCRIPTION ON THE FACE HEREOF. THERE IS NO EXPRESS OR IMPLIED WARRANTY OF MERCHANTABILITY OR A WARRANTY OF FITNESS FOR A PARTICULAR PURPOSE. ADDITIONALLY, THIS WARRANTY IS IN LIEU OF ALL OTHER OBLIGATIONS OR LIABILITIES ON THE PART OF NAPCO.

Any action for breach of warranty, including but not limited to any implied warranty of merchantability, must be brought within the six months following the end of the warranty period.

IN NO CASE SHALL NAPCO BE LIABLE TO ANYONE FOR ANY CONSEQUENTIAL OR INCIDENTAL DAMAGES FOR BREACH OF THIS OR ANY OTHER WARRANTY, EXPRESS OR IMPLIED, EVEN IF THE LOSS OR DAMAGE IS CAUSED BY THE SELLER'S OWN NEGLIGENCE OR FAULT.

In case of defect, contact the security professional who installed and maintains your security system. In order to exercise the warranty, the product must be returned by the security professional, shipping costs prepaid and insured to NAPCO. After repair or replacement, NAPCO assumes the cost of returning products under warranty. NAPCO shall have no obligation under this warranty, or otherwise, if the product has been repaired by others, improperly installed, improperly used, abused, altered, damaged, subjected to accident, nuisance, flood, fire or acts of God, or on which any serial numbers have been altered, defaced or removed. NAPCO will not be responsible for any dismantling, reassembly or reinstallation charges, environmental wear and tear, normal maintenance expenses, or shipping and freight expenses required to return products to NAPCO. Additionally, this warranty shall not cover scratches, abrasions or deterioration due to the use of paints, solvents or other chemicals.

This warranty contains the entire warranty. It is the sole warranty and any prior agreements or representations, whether oral or written, are either merged herein or are expressly cancelled. NAPCO neither assumes, nor authorizes any other person purporting to act on its behalf to modify, to change, or to assume for it, any other warranty or liability concerning its products.

In no event shall NAPCO be liable for an amount in excess of NAPCO's original selling price of the product, for any loss or damage, whether direct, indirect, incidental, consequential, or otherwise arising out of any failure of the product. Seller's warranty, as hereinabove set forth, shall not be enlarged, diminished or affected by and no obligation or liability shall arise or grow out of Seller's rendering of technical advice or service in connection with Buyer's order of the goods furnished hereunder.

NAPCO RECOMMENDS THAT THE ENTIRE SYSTEM BE COMPLETELY TESTED WEEKLY.

**Warning:** Despite frequent testing, and due to, but not limited to, any or all of the following; criminal tampering, electrical or communications disruption, it is possible for the system to fail to perform as expected. NAPCO does not represent that the product/system may not be compromised or circumvented; or that the product or system will prevent any personal injury or property loss by burglary, robbery, fire or otherwise; nor that the product or system will in all cases provide adequate warning or protection. A properly installed and maintained alarm may only reduce risk of burglary, robbery, fire or otherwise but it is not insurance or a guarantee that these events will not occur. CONSEQUENTLY, SELLER SHALL HAVE NO LIABILITY FOR ANY PERSONAL INJURY, PROPERTY DAMAGE, OR OTHER LOSS BASED ON A CLAIM THE PRODUCT FAILED TO GIVE WARNING. Therefore, the installer should in turn advise the consumer to take any and all precautions for his or her safety including, but not limited to, fleeing the premises and calling police or fire department, in order to mitigate the possibilities of harm and/or damage.

NAPCO is not an insurer of either the property or safety of the user's family or employees, and limits its liability for any loss or damage including incidental or consequential damages to NAPCO's original selling price of the product regardless of the cause of such loss or damage.

Some states do not allow limitations on how long an implied warranty lasts or do not allow the exclusion or limitation of incidental or consequential damages, or differentiate in their treatment of limitations of liability for ordinary or gross negligence, so the above limitations or exclusions may not apply to you. This Warranty gives you specific legal rights and you may also have other rights which vary from state to state.